FROST & SULLIVAN

Digital Security and Paperless Transformation Market

CONTENTS

1. Global Macroeconomic Trends

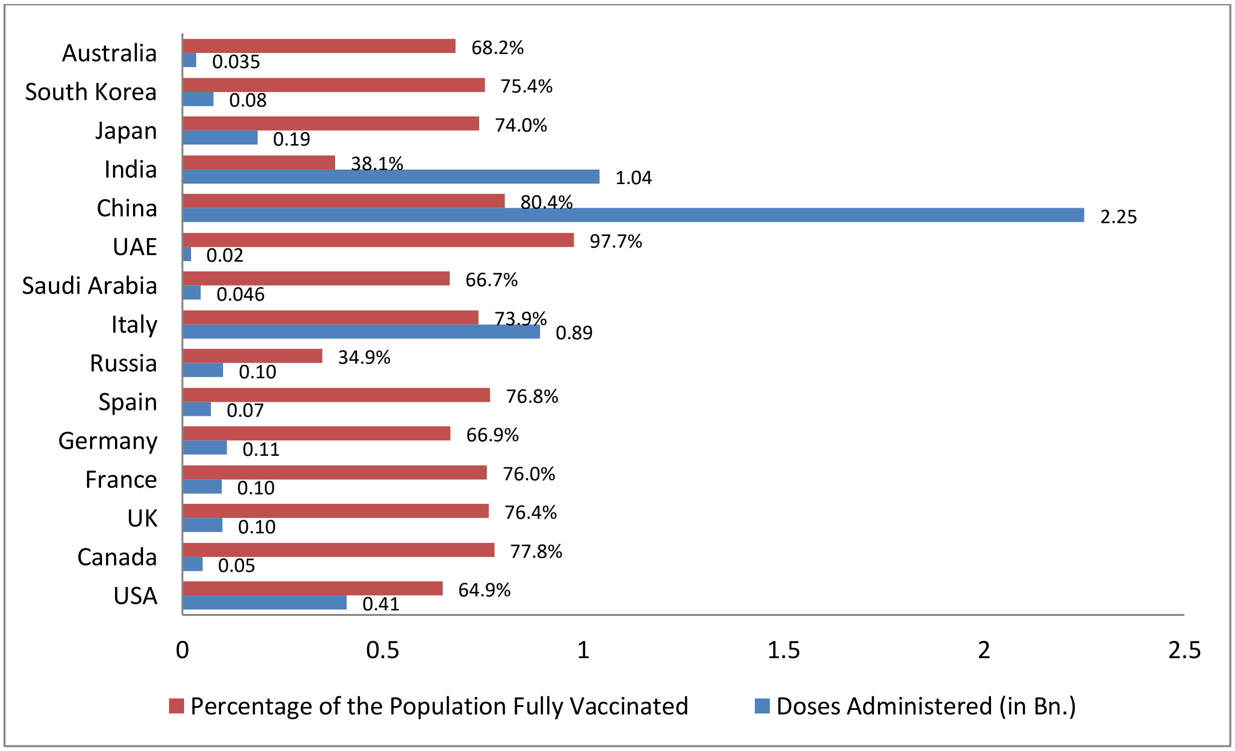
The COVID-19 pandemic has been the biggest headline for 2020 and most part of 2021. Every country on the global map was affected due to the corona virus with deaths recorded over 4.9 million as on date (28th October 2021). The existence of human life was threatened as people feared for their lives and stayed back at homes. Economic activity saw a grinding halt due to countries declaring nationwide lockdown for several months. Enterprises declared unprecedented losses thereby affecting GDP growth.

While the pandemic has surely been painful for all, it has helped people to think differently. It has become a catalyst for change, where innovations and newer concepts gained center stage. Governments brainstormed with economists, strategists and technologists on finding solutions and ways to boost the economy. The COVID-19 vaccine developed in late 2020 has certainly been the light after passing through a phase of darkness. Now, as we stand in the last quarter of 2021, business confidence among decision makers and entrepreneurs have certainly improved and the business sentiment remains positive.

1.1 Global Economic Outlook

The COVID-19 vaccine has been the strongest enabler for controlling the number of daily cases worldwide. While the world can still be divided into 2 sets: countries that look towards opening up the economy and normalization of business activity (predominantly the advanced economies) and those who see rise in daily cases of infection and death tolls, the sign of recovery cannot be termed as "end of the pandemic". Cases could spike up anytime bringing back harsh controlled measures once again.

Figure 1: Vaccine Doses Administered andPercentage of the Population Completely Vaccinated



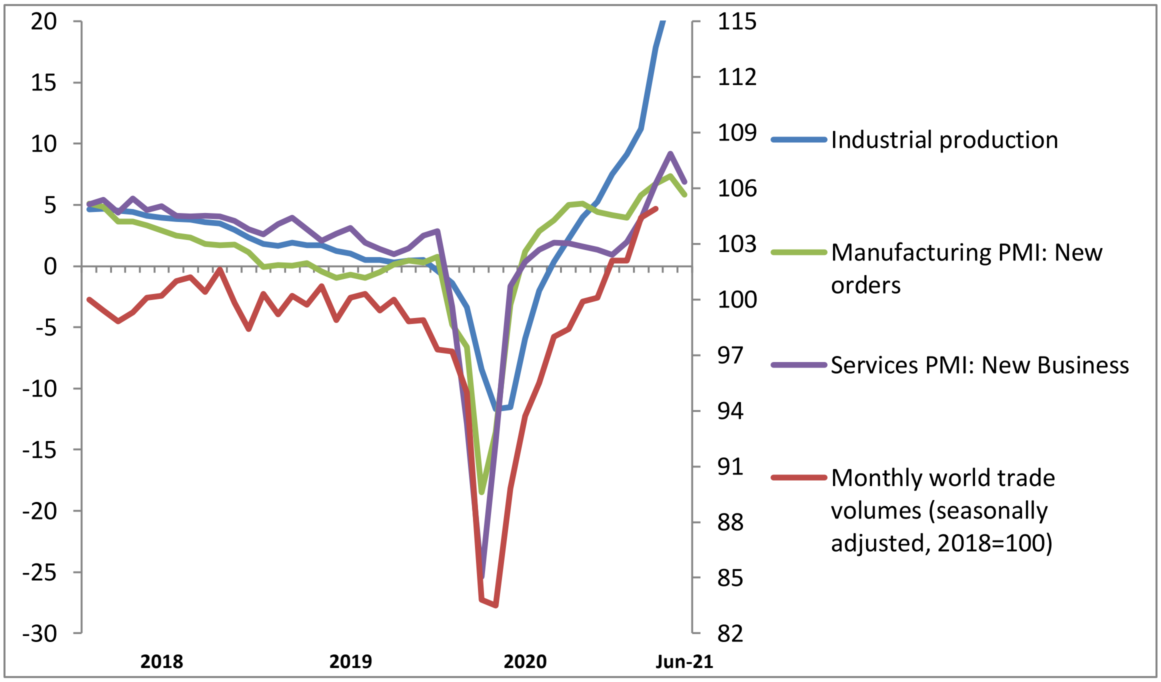
Source: Bloomberg.com, data as on 28th October 2021 (9:04 AM IST)

State of the Economy

In the current state of economy, the IMF (International Monetary Fund) has projected a growth of 5.9% in 2021 and 4.9% in 2022 as per the October 2021 "World Economic Outlook Growth Projections". The 2021 global forecast has decreased slightly from what it was in April 2021 WEO (World Economic Outlook). Prospects for emerging and developing countries (especially for some of the emerging Asian countries) have been marked down for 2021. In contrast, the outlook for developing countries is revised up. These revisions are based on improved pandemic situations and changes in government policies.

Figure 2: Global Activity Indicators

(Three-month moving average, annualized percent change; deviations from 50 for PMIs, unless noted otherwise)



Source: CPB Netherlands Bureau for Economic Policy Analysis, Haver Analytics, Markit Economics, and IMF staff estimates

Note: PMI above 50 indicates expansion while below 50 indicates contraction, PMI = purchasing managers' index

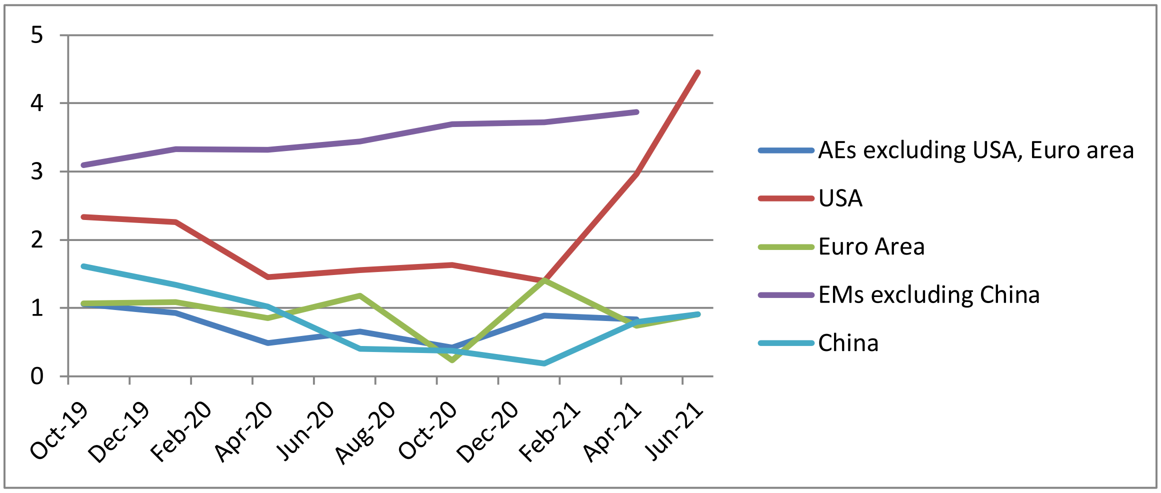
Inflation

The recent rise in prices, by and large, reflects unusual pandemic related developments and transitory demand-supply mismatches. Inflation is expected to settle down with pre-pandemic ranges in most of the countries in 2022 except for some of the emerging markets and developing economies (mostly due to rise in food prices). In some emerging market and developing economies in sub-Saharan Africa, Middle East and Central Asia, there has been a significant rise in food prices due to food crisis and rise in global food prices. Currency depreciation has added onto the worry and raised prices of imported goods. Core inflation, which removes the influences of energy and food prices, however have remained contained for most part (please refer to the figure given below). The rise in core inflation in USA (driven by increased prices of used cars, lumber, and air travel) also reflects pandemic related disruptions rather than a rapid exhaustion of spare capacity.

It is mostly likely that inflation would subside down to its pre-pandemic ranges in 2022 once the transitory disturbances settle down. However, in some pockets of the emerging and developing economy, food price pressures and higher oil prices would continue specifically from importers.

Figure 3: Core Inflation

(annual percentage change)



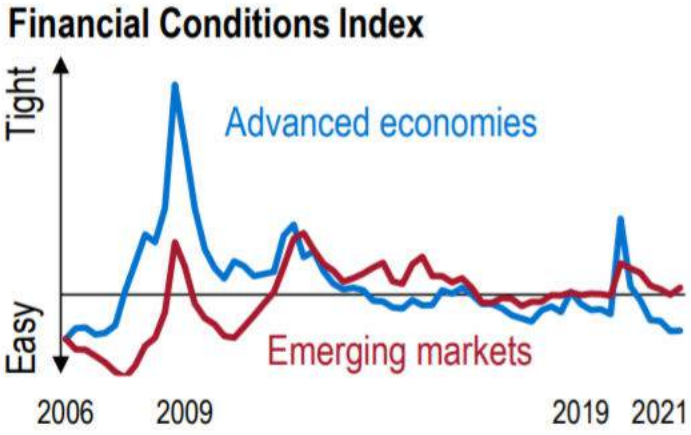
Source: Haver Analytics; and IMF staff calculations

Note: AEs = advanced economies, EMs = emerging market economies

Global Financial Conditions

In the larger context, global financial conditions have eased up and have remained supportive of growth despite the negative impact of the COVID-19 pandemic on GDP and fears of higher inflation turn out. Countries like USA have improved financial conditions reaching levels similar to the pre-pandemic days. Rising equity valuations, tighter credit spreads, and rapidly climbing house prices remain the growth drivers and indicators of improving economy. For emerging market economies, improvement has been slow (in general) as monetary policy tightening in several countries has offset gains in asset prices.

Figure 4: Financial Conditions Index



Source: Global Financial Stability Report, IMF, October 2021

1.1. GDP Growth Outlook

Globally, the total number of COVID-19 cases and transmission is expected to go down substantially by the end of 2022. Precautionary measures and improved coverage of vaccine distribution would be fundamental. The advanced countries are expected to reach vaccine availability by summer of 2021. Some of the emerging economies would have better accessibility to the vaccine by the end of this year. Remaining ones would have access by end of 2022. Summarily, major regions of the world would have vaccine availability by end of next year – which becomes critical for the GDP growth of each country.

Figure 5: Overview of the World Economic Outlook Projections
(real GDP, annual percent change)

	2020	2021*	2022*
World Output	**-3.1**	**5.9**	**4.9**
Advanced Economies	**-4.5**	**5.2**	**4.5**
United States	**-3.4**	**6.0**	**5.2**
Euro Area	**-6.3**	**5.0**	**4.3**
Germany	-4.6	3.1	4.6
France	-8.0	6.3	3.9
Italy	-8.9	5.8	4.2
Spain	-10.8	5.7	6.4
Japan	**-4.6**	**2.4**	**3.2**
United Kingdom	**-9.8**	**6.8**	**5.0**
Canada	**-5.3**	**5.7**	**4.9**
Other Advanced Economies	**-1.9**	**4.6**	**3.7**
Emerging Market and Developing Economies	**-2.1**	**6.4**	**5.1**
Emerging and Developing Asia	**-0.8**	**7.2**	**6.3**
China	2.3	8.0	5.6
India	-7.3	9.5	8.5
ASEAN-5	**-3.4**	**2.9**	**5.8**
Emerging and Developing Europe	**-2.0**	**6.0**	**3.6**
Russia	-3.0	4.7	2.9
Latin America and the Caribbean	**-7.0**	**6.3**	**3.0**
Brazil	-4.1	5.2	1.5
Mexico	-8.3	6.2	4.0
Middle East and Central Asia	**-2.8**	**4.1**	**4.1**
Saudi Arabia	-4.1	2.8	4.8
Sub Saharan Africa	**-1.7**	**3.7**	**3.8**
Nigeria	-1.8	2.6	2.7
South Africa	-6.4	5.0	2.2
Memorandum			
Emerging Market and Middle Income Economies	**-2.3**	**6.7**	**5.1**

Low Income Developing Countries	**0.1**	**3.0**	**5.3**

*Projected

Note: For India, data and forecasts are presented on a fiscal year basis, with FY 2020/21 starting in April 2020. For the October 2021 WEO, India's growth projections are 8.3% in 2021 and 9.6% in 2022 based on calendar year.

Source: IMF, World Economic Outlook Update, October 2021

The world GDP grew at 2.8% in 2019, a year before the pandemic hit. Devastating impact of the pandemic pushed the GDP to negative 3.1% - first time since quite a while in 2020. A strong rebound of the world economy is expected in 2021 with growth projected at 5.9% and 4.9% in 2021 and 2022 respectively. Strong fiscal and monetary support from the central governments along with within-level inflation rates would help either to improve the growth estimates or maintain the growth projections.

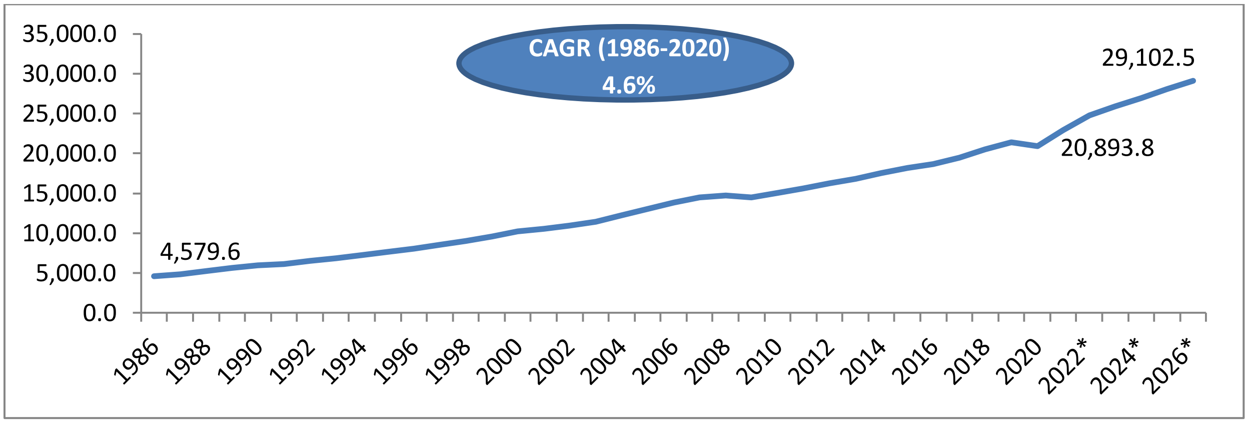
- **Advanced Economies:** After a dip in the GDP by -4.5% in 2020, strong growth is expected in 2021 and 2022. Growth projections have been revised up from 2021-22 from the earlier projections due to the better outlook in the 2nd half of 2021. The US economy has improved significantly along in the last few months specifically due to infrastructure investment and expected strengthening of the social safety in the 2nd half of 2021. Projections for Japan have been downgraded in 2021 due the rise in COVID cases and lockdown restrictions during the first half of the year. However, Japan is anticipated to see strong growth in the 2nd half of 2021 as vaccination rate improves and the economy opens up. Similar growth momentum is expected from countries like France, Germany, Italy, and Spain in the following months rolling into 2022.
- **Emerging and Developing Economies:** The emerging and developing economies include countries like China, India, Russia, Brazil, Mexico, Saudi Arabia, Nigeria, and South Africa. China is one of the very few countries that experienced growth even during 2020. 8.0% GDP growth is expected in 2021 followed by 5.6% in 2022. Growth prospects for India also improved after the country battled the second wave of the pandemic between March and May. The current situation looks far better as COVID cases are under control expect for some specific regional clusters. However, a possible third wave of the pandemic could worsen the situation once again. Similar dynamics work for the ASEAN-5 group (Indonesia, Malaysia, Philippines, Thailand, Vietnam) which has seen a recent spike thereby dragging the lull economic period. For positive economic sentiments in Brazil and Mexico has pushed forward the growth projections in Latin America. Even for Middle East and Central Asia, projections have been upgraded (economic boost from Morocco and Pakistan). Saudi Arabia took a hit in the projections due to subdued oil productions below the OPEC+ quota earlier this year.
- **Low Income Developing Countries:** This set of countries managed to have a flat growth in 2020. The impact of the COVID-19 pandemic was not severe and hence did not impact the respective economies. Growth is expected to be in low single digits in 2021 and 2022. However, IMF estimates that the low income developing countries would need ~$200 Bn. in spending to combat the pandemic and an additional $250 Bn. to regain their pre-pandemic growth numbers. Labor market prospects for low skilled workers and youth continue to remain weak, increased gap of gender inequality noticed. Unemployment rates are higher than earlier which pushes towards poverty. Estimates suggest, ~80 million additional people are expected to enter extreme poverty during 2020-21 as compared with pre-2020 numbers.

1.2. GDP Growth of Select Economies

United States of America

Figure 6: GDP of United States of America ($ Bn.) (1986 – 2026)

(at current prices)



*Base Year is 2020, Projected from 2021 onwards

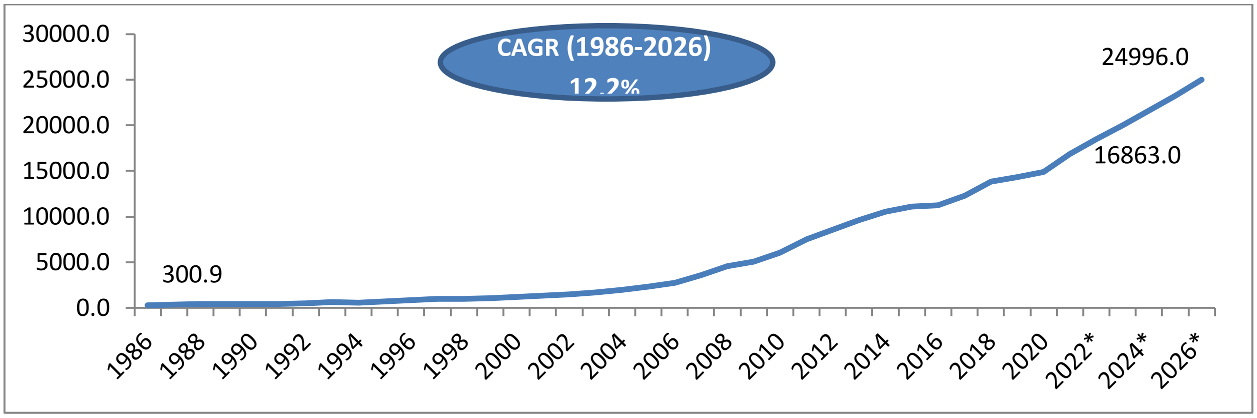
Data labels mentioned above in the graph are for 1986 (historical data), 2020 (base year), and 2026 (end of forecast period)

Source: IMF, Oct 2021

The US economy increased over 4.5 times in the last 35 years. GDP grew at a steady rate at a CAGR of 4.6% since 1986. It is currently the largest economy in the world. While, it is often been said that China would surpass US in terms of GDP by 2030, there is still a significant difference among the two countries. The country is technologically powerful and has remained as a center of innovation. It has been the home to few of the world's biggest companies. US dollar is considered as universal and used in most international transactions. The country has a strong trading partnership with global and regional powerhouses like China, EU, Canada, Mexico, India, Japan, South Korea, UK and Taiwan. The oldest democracy is the world's largest importer and second largest exporter. Free trade agreements have been signed with several countries that include USMCA, Australia, South Korea, Israel, and several other thereby boosting bi-lateral trades.

China

Figure 7: GDP of China ($ Bn.) (1986 – 2026)
(at current prices)



*Base Year is 2020, Projected from 2021 onwards

Data labels mentioned above in the graph are for 1986 (historical data), 2020 (base year), and 2026 (end of forecast period); CAGR from 1986 till 2020

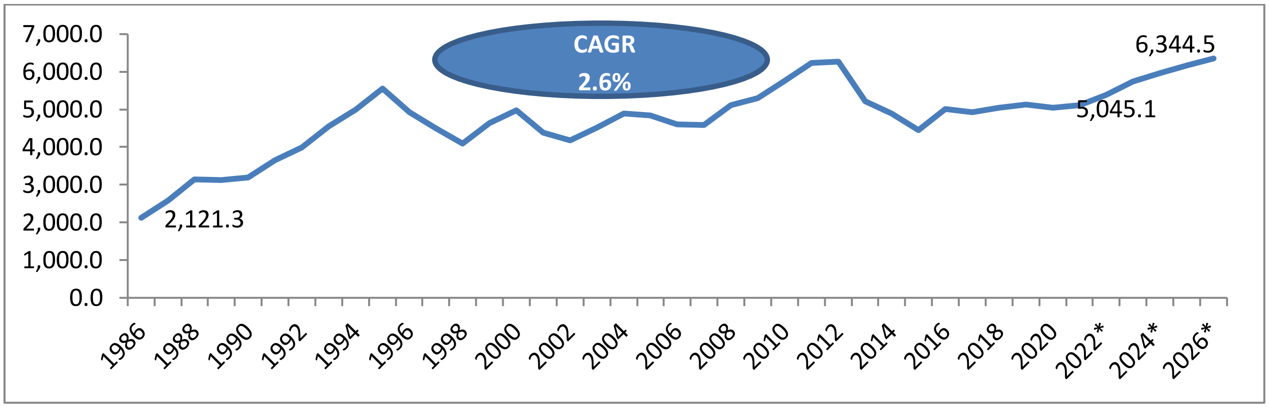
Source: IMF, Oct 2021

China is one of the fastest growing economies of the world. The country remains mostly controlled by the government as state-owned enterprises account for 60% of China's market capitalization as on 2019. The growth story for the country started in 1978 under the leadership of Deng Xiaoping. This has resulted in making China, the fastest growing major economy; with grow rates even crossing 10%. Shanghai, Hong Kong, Beijing, and Shenzhen are among the top financial centers of the country contributing significantly towards the country's financial health. GDP per capita has increased steady for the world's second largest economy has increased exponentially over the years. As of 2019, GDP per capita stands at $10,242.92 and expected to become $17, 003.09 by the end of 2026. From an agriculture and industry led economy, China is fast becoming a services led economy. Currently, the services industry accounts for over 50% of the economy as against 44.2% in 2010. Over the last 2 years, the inflation rate has decreased from 2.9% in 2019 to 2.5% in 2020 and expected to reduce even further to 1.19% by the end of the current year.

Japan

Figure 8: GDP of Japan ($ Bn.) (1986 – 2026)

(at current prices)



*Base Year is 2020, Projected from 2021 onwards

Data labels mentioned above in the graph are for 1986 (historical data), 2020 (base year), and 2026 (end of forecast period); CAGR from 1986 till 2020

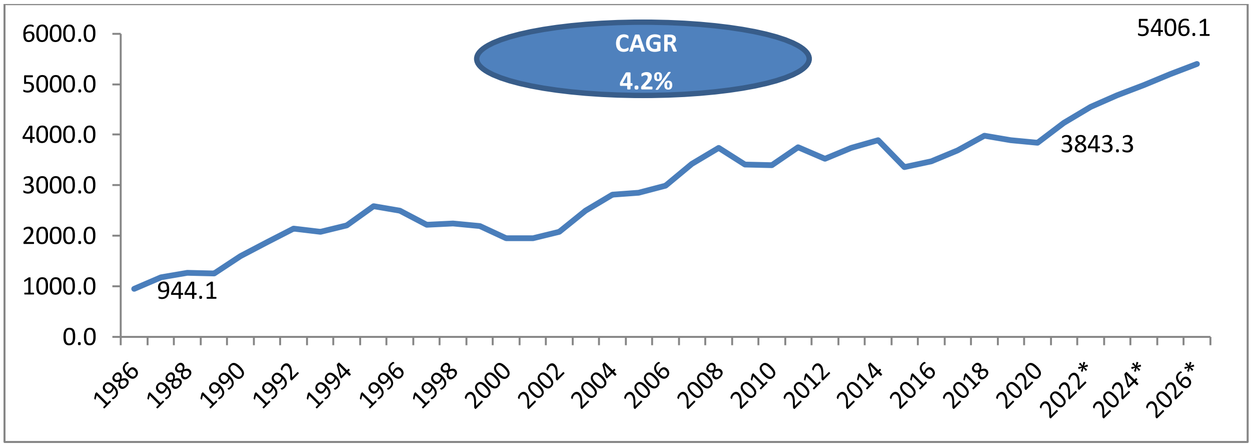
Source: IMF, Oct 2021

The Japanese economy is currently valued at $5045.1 Bn. (in 2020) and expected to reach $6344.5 Bn. by the end of 2026. The growth has not been very smooth like USA or China but has seen economic stagnation during the course of the period. The country is considered as a highly developed free-market economy. Japan ranks 3rd in the world by nominal GDP and fourth largest by purchasing power parity (PPP). The automobile and electronics sector has been among the world's largest. From optical instruments, hybrid vehicles to robotics; Japan has been the manufacturing hub for high-tech and precision goods. However, the country has been facing stiff competition from regional players like South Korea and Taiwan in the recent past. As of 2021, Japan has significantly higher level of debt when compared with other developed nations, standing at 266% of the GDP. The Tokyo Olympics could have been a revenue booster the country, however strict restrictions and spectator free games has been a damper. The Japanese economy currently faces considerable challenges from the ageing population which could be a road-block in the country's growth story.

Germany

Figure 9: GDP of Germany ($ Bn.) (1986 – 2026)

(at current prices)



*Base Year is 2020, Projected from 2021 onwards

Data labels mentioned above in the graph are for 1986 (historical data), 2020 (base year), and 2026 (end of forecast period); CAGR from 1986 till 2020

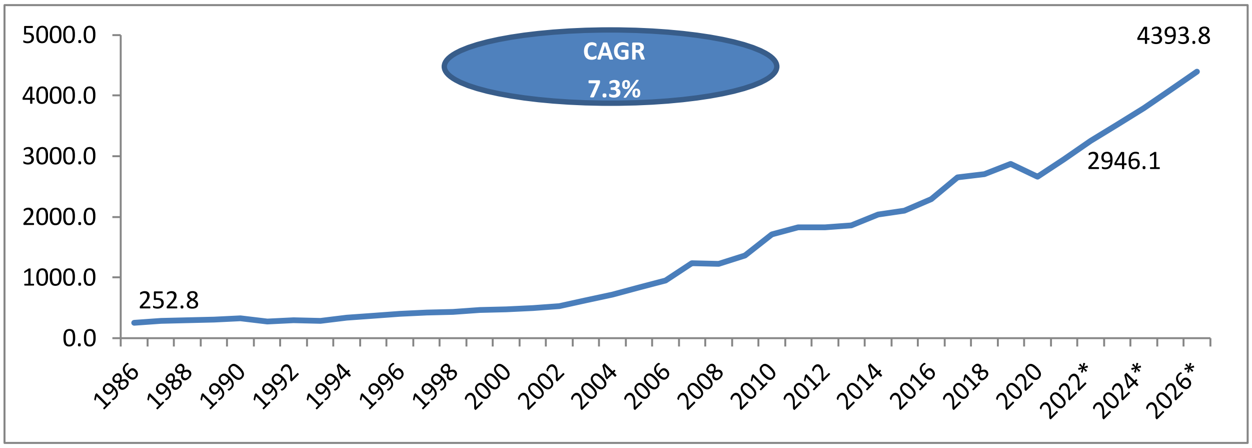
Source: IMF, Oct 2021

Germany is one among the top 5 economies of the world. The country's GDP currently stands at $3843.3 Bn. and expected to reach $5406.1 Bn. by the end of 2026. The economy has grown at a CAGR of 4.2% since 1986. Stronger growth is expected at 5.9% till 2026. A home to few of the world's most renowned car manufacturers (Daimler, Volkswagen and BMW), the revenue contribution to the country's GDP is prominent. 53 out of the world's 2000 largest publicly listed companies (measured in terms of revenue) are he/adquartered in Germany. Mineral and wood availability (timber, lignite, potash and salt) in the country is also high making the country rich in natural resources. Cities like Berlin, Hanover, Frankfurt, Cologne, Leipzig and Düsseldorf remain as strong growth centers for the country.

India

Figure 10: GDP of India ($ Bn.) (1986 – 2026)

(at current prices)



*Base Year is 2021, Projected from 2022 onwards

Data labels mentioned above in the graph are for 1986 (historical data), 2021 (base year), and 2026 (end of forecast period); CAGR from 1986 till 2021

Source: IMF, Oct 2021

India has been one of the fastest growing emerging economies much ahead of advanced economies like Germany, Japan and USA. The growth has specifically picked up after the 1991 economic reform and after 2000 with the .com boom in India. Except for one or two instances (the global recession of 2008 and economic impacts in 1993), the country's economy has grown at healthy double digits. The COVID-19 pandemic had a strong negative impact on the growth, much in-line with the global sentiments, with de-growth registered at -7.3%. By the end of FY 2021, the Indian economy stood at 2946.1 Bn. and expected to reach 4393.8 Bn. by the end of FY 2026. GDP growth is expected to be in the range of 8.3% (at an even faster rate than the historic growth) from FY 2021 till FY 2026.

The long term growth perspective of the Indian economy looks positive due to the country's young population and increasing interest towards globalization. Around 60% of the country's GDP is driven by the domestic private consumption. USA, China, UAE, Saudi Arabia, Switzerland, Germany, Hong Kong, Indonesia, South Korea, and Malaysia are the ten largest trading partners for India. A significant portion of India's GDP comes from the service sector while industrial and agriculture employs majority of the labor force.

In addition to the organic growth opportunities that lie, enterprises that have strong focus on international markets would benefit from the falling rupee. $1 was valued at INR. 12.37 in 1985 which is currently valued at INR. 74.99 on the last working day of October 2021. Strong export volumes would bring in better revenue numbers for enterprises.

1.3. Digital growth levers to GDP Growth

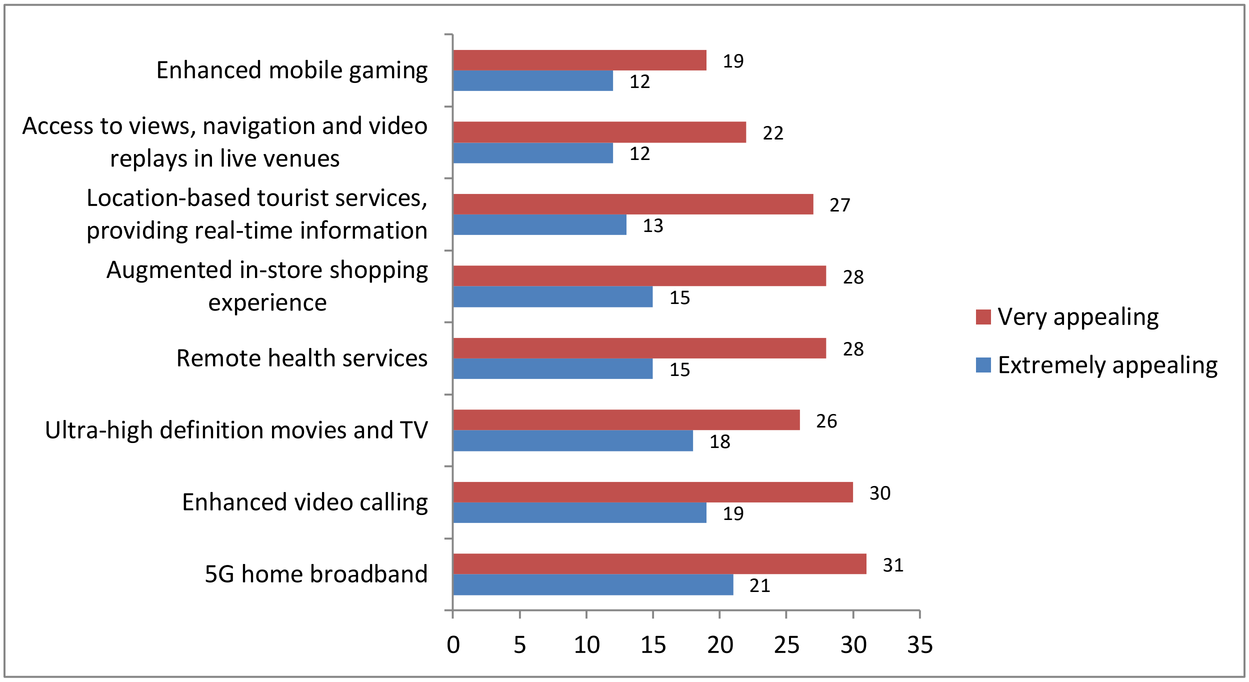
Global

Countries that have a strong digital foot-print has been at the forefront of growth. To remain ahead in the race of global dominance, countries cannot afford to not take a digital first strategy. With the numerous advantages that digital provides over manual, digital transformation has become the backbone of an economy. Digital economy is the economic activity that results from billions of everyday online connections among the citizens (people), businesses, devices, entities, data, and processes. Connectivity remains prime which means connecting people, organizations, and machines that result from the internet, mobile technology and IoT. Also known as the internet economy, digital economy helps execute existing/mundane tasks more easily with the use of technologies which other-wise becomes far more tiring and time consuming. Digital economy is not just digitlization or automation but takes cognizance of technologies and platforms like hyperconnectivity, IoT, big data, analytics, wireless networks, mobile devices and social media.

- **Hyperconnectivity:** First used by Barry Wellman and Anabel Quan-Haase to describe the evolving state of communications in society, hyperconnectivity refers to connectivity that exists in the digital world and enables the interaction between information systems, data and devices – all of them connected through a single thread of internet. A hyperconnected infrastructure includes all kinds of electronic and computer devices like PCs, PDAs, cellular phones, television receivers, personal radios, GPS systems and more. In the modern-day world, hyperconnectivity includes IoT devices, voice assistants, browsers and 5G networks.

5G is expected to be revolutionary for the future. It would find use cases in smart cities, connected vehicles, industrial IoT, feet management, logistics and more. 5G's super performance, achieved through higher frequency waves, small cells, and beam forming technology makes it highly reliable with low latency communication for high and low bandwidth applications. Low latency is the key and it could be well achieved with the use of 5G communication.

Figure 11: 5G use cases and their appeal for global consumers, 2020



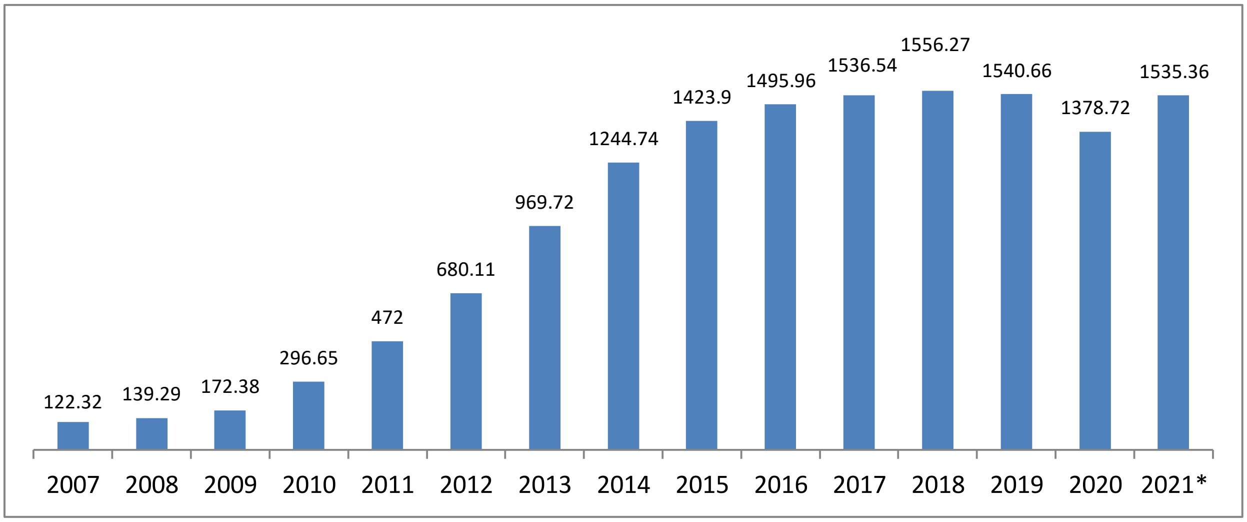
Source: The Mobile Economy Report 2021, GSMA

- **Internet of Things (IoT):** IoT is considered as one of the fundamental pillars of digital transformation since it enables and accelerates business creation and opportunities with an aim to ease up work, enable better efficiency, and improve the way of living. IoT has often been an element of change in the industrial and consumer technology. SCADA systems, ICS, and sensors have IoT applications which have become part of the Industry 4.0 concept. Each of these devices collect and transfer volumes of data through a network to generate actionable insight critical for decision making. Edge devices are a strong use case for IoT which would accelerate digitization.
- **Big Data and Analytics:** Most electronic devices generate humongous amount of data that needs to be used for extracting meaningful insights. The unstructured data needs to be cleaned and processed to deliver fact based decision making. Businesses use big data analytics to better understand customers, develop targeted marketing messages, launch new products, check ideas, improve business processes, and optimize customer journeys. Economies cannot embark in the digitization journey if an ecosystem to churn the citizen data cannot be churned out.
- **Wireless Networks:** As per definition, wireless network is a network arrangement where the device stays connected to the network despite taking the device all around wherever the user wishes to move. The device does not remain connected with a wire or a cable of any kind. The

computer network makes use of radio frequency (RF) connections between nodes in the network. In a digital economy, consumers can connect to a public wifi and perform digital transaction, search online or browse social media sites.

- **Mobile Devices:** With the consumerization of IT, mobile devices have become a part and parcel of our daily lives. Mobile devices enable people to connect to wireless networks and perform online tasks. Digital payments have reached newer heights and mobile phone have become the fundamental device for transactions. Different mobile applications, developed by governments and private entities, have come up making human lives much easiler – from food delivery apps to shopping, cab booking, mobile banking, and maps – all delivered through an app.

Figure 12: Global Smartphone Sales (in Mn. Units), 2007-2021



*Projected
Source : Statista

India

Over the last 6 years, India has been riding growth specifically on digital initiatives. The Digital India campaign has been pivotal to the country's digital focus that has seen significant traction. The Digital India program is a flagship program by the Government of India with a vision to transform India into a digitally empowered society and knowledge economy. Launched by the Government of India and coordinated by Meity (Ministry of Electronics and IT) in July 2015, the Digital India campaign has a vision to ensure that government services are being made available to citizens electronically by reducing paperwork. The campaign also has a plan to connect rural India with high speed connectivity (internet). The Prime Minister of India remains as the Chairman of the monitoring committee.

Figure 13: Vision of Digital India

Digital Infrastructure as a Core Utility to Every Citizen	Governance & Services on Demand	Digital Empowerment of Citizens
Availability of high speed internet as a core utility for delivery of services to citizens Cradle to grave digital identity that is unique, lifelong, online and authenticable to every citizen Mobile phone & bank account enabling citizen participation in digital & financial space Easy access to a Common Service Centre Shareable private space on a public cloud Safe and secure cyber-space	Seamlessly integrated services across departments or jurisdictions Availability of services in real time from online & mobile platforms All citizen entitlements to be portable and available on the cloud Digitally transformed services for improving ease of doing business Making financial transactions electronic & cashless Leveraging Geospatial Information Systems (GIS) for decision support systems & development	Universal digital literacy Universally accessible digital resources Availability of digital resources / services in Indian languages Collaborative digital platforms for participative governance Citizens not required to physically submit Govt. documents / certificates

Source : Digitalindia.gov.in

The Digitial India initiative rests on 9 key pillars:

1. Broadband Highways
2. Universal Access to Phones
3. Public Internet Access Program
4. E-Governance
5. eKranti – Electronic delivery of services
6. Information for All
7. Electronic Manufacturing – Target net zero imports
8. IT for Jobs
9. Early Harvest Programs

In order to boost the Information and Communications Technology (ICT) infrastructure of the country, the Government of India has taken the following key initiatives:

BharatNet

Aim to provide broadband access to 250000 gram panchayats through a network of Optical Fibre Cable

Smart Cities

Creation of 100 smart cities and allocation of INR. 1000 crore for a period of 5 years

Common Service Centre (CSC)

CSCs are centres through which e-governance and related services will be made available to villages

Digitization of Post Offices

Including setting up centralized data centers, networking of all post offices and enabling digital payments

Universal Access to Mobile Connectivity

Covering 42,300 uncovered villages through universal mobile connectivity in the country

Further to the ICT infrastructure campaigns, the India government has taken several initiatives as a part of the Digital India program :

eSign: eSign framework allows for online digital signature by leveraging Aadhaar and other forms (PAN, Bank KYC, etc.) of authentication

eInvoicing: To make invoices go paperless and bring standardization in reporting/tax collection

eStamping: Conducted through NeSL which is a govenment body constituted under Indian Bankruptcy Code to enable completely digital contracting

National Center of Geo-informatics: GIS platform is used for sharing and collaborating GIS data source, location-based analytics and decision support system

Information Security Education and Awareness (ISEA) Phase II & Cyber Security: Capacity building in the area of Information Security to address the human resource requirement, training and develop information security awareness

MyGov app: Citizen centric platform empowering people to connect with the government & contribute towards good governance

DigiLocker: Digital Locker facility provides citizen a shareable private space on a public cloud and making all documents/certificates available on the cloud

Swachh Bharat Abhiyaan app: To further the Swachh Bharat mission, the government has launched this app which will be used by people and government organizations

National Scholarship Portal (NSP): One-stop solution for end-to-end scholarship process right from the submission of student application, verification, sanction and disbursal to end beneficiary for all the scholarships provided by the Government of India

Wi-fi Hotspots: Under the initiative, the government plans to deploy Wi Fi at public and tourist places

India Post Payments Bank: Known as IPPB, it is a specialized division of Indian Post which is under the jurisdiction of the Department of Post a department under Ministry of Communications of the Government of India

PayOnline Launch of ePayment Portal: National ePayment gateway is enabling every Indian citizen to make online payments for all Government based transactions, ecommerce payments and other related tasks

Launch of Online labs for schools: Under this nationwide initiative, online labs will be available in Hindi, Malayalam and Marathi and offered in both urban and rural schools 30,000 teachers in all Indian states will be provided training on online labs

eEducation: Providing high-tech education in remote and urban areas using technology like smartphones, apps and Internet services

e-Hospital: An initiative of Digital India that has made it easy for the citizens to take appointments in major hospitals

Digital MSME: An ICT initiative launched in the MSME (micro, small & medium enterprises) sector to help adopt ICT tools and applications in their production and business process

TReDS: An electronic platform for facilitating the financing / discounting of trade receivables of Micro, Small and Medium Enterprises (MSMEs) through multiple financiers

The Government of India has taken up 44 mission mode projects under the e-Kranti scheme with centre-state partnership (in some cases) with the vision of transforming e-Governance with a view to enable presenceless, paperless and cashless delivery of services. The e-Kranti scheme has a potential of 400 Mn. eSignatures.

Centre (15)	State (17)	Integrated (12)
• Banking • Insurance • Income Tax • Central Excise • MCA 21 • Pensions • Passport • National ID/UID • Immigration / Visa • E-office • Posts • Central Armed Paramilitary Forces • e-Bhasha • NMEICT • e-Sansad	• Transport • Land Rec./NLRMP • e-District • Commercial Taxes • Treasuries • Municipalities • Agriculture • PDS • Employment Exchange • Education • Health • e-Panchayat • CCTNS • Agriculture 2.0 • E-Vidhaan • Rural Development • Women & Child Development	• India Portal • NSDG • CSC • Financial Inclusion • e-Trade • e-Courts • e-Procurement • e-Biz • NGIS • Road and Highway Information System • Social Benefits • Urban Governance

1.4. Role of Digital Solutions in the Current Scenerio

The rise of COVID-19 resulted in governments imposing social distancing norms and lockdowns. This forced organizations to move to "Work from Home" resulting in the need for adoption of digital solutions that facilitated remote fulfillment of transactions. Use of digital solutions peaked during the pandemic and helped contain the spread of the virus as people did not have the need to physically visit places. People started using online applications for making payments, filling up and signing forms, and transact online to avoid cash or submit forms. Paperless soutions experienced huge spike in demand for signing documents and is expected to stay for long as digital becomes the future.

eSign is one of the most important digital and paperless solutions. The Indian government has been laying strong focus on e-Sign which is part of the Digtal India campaign. eSign is an online electronic signature service which can be integrated with service delivery applications via an open API to facilitate an Aadhaar holder/eKYC compliant to digitally sign a document. It is an innovative initiative for allowing easy, efficient and secure signing of electronic documents by authenticating signer using e-KYC services.

By using this service, a user can digitally sign an electronic document without the need to obtain a physical digital signature dongle. Application Service Providers (ASPs) can integrate the eSign API with their application to enable a user to sign electronic forms or documents. Government agencies, Banks, Financial Institutions and Educational Institutions are the major use of eSign services. Some of the most common uses-cases of eSign include:

Department	Purpose
Tax	Application of ID, e-filing, GST
Financial Sector	Application for account opening in banks and post office
Transport Department	Application for driving licence renewal, vehicle registration
Government Agencies	Application for birth, caste, marriage, income certificate etc
Passport	Application for issuance, reissue
Telecom	Application for new connection
Educational	Application forms for course enrollment and exams
Parliament	Submission of parliament questions by menbers of the Parliament
Digital Locker	Self attestation

Digital Enablers

Aadhaar

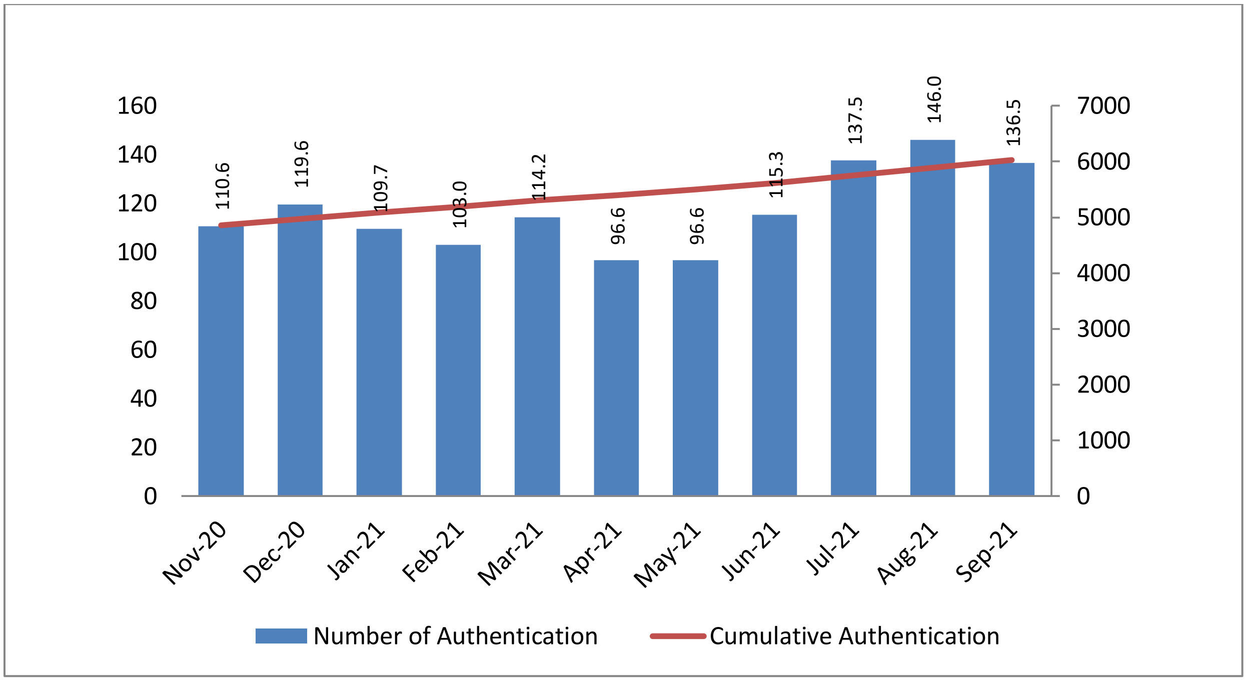
Aadhaar is a 12 digit unique identification number issued by the Government of India to every Indian resident. The Unique Identification Authority of India (UIDAI) is the statutory body behind the program which functions under the Ministry of Electronics and Information Technology. Aadhaar is primarily used as a sole identification proof and serves as a basis for KYC (know your customers) norms used by banks, financial institutions, telecom operators, income tax and GST, and other businesses that maintain customer profiles. In a recent move, the Indian government has asked its citizens to link Aadhaar with PAN, Ration Card, Banks Accounts, etc.

eSign has a strong relevance for online electronic signatures. eSign facilitates Aadhaar holders to digitally sign a document by using eSign services provided by Certifying Authorities (CAs). The unique identity card holders can sign documents using biometric or one time password (OTP) as a part of digital authentication which does not require any paper based application or document. Authentication of the signer is carried out by e-KYC services of UIDAI. Application Service Providers (ASPs) use Open APIs to easily integrate e-Sign facility into their applications which enables them to accept legally valid and non-repudiable digitally signed documents.

Total Population of India	Number of Aadhaar Assigned	Saturation %
1,361,343,000	1,252,847,789	92.03%

Source : Uidai.gov.in, data as on 31st Aug 2021, population estimated by August end

Figure 14: Aadhaar Authentication Trend (in Crs.), Nov 2020 – Sep 2021



Source : Uidai.gov.in

PAN

Permanent Account Number or PAN is a ten digit unique alphanumeric number issued by the Income Tax Department that enables the department to identify/link all transactions of the PAN holder. The PAN card is linked to the Aadhaar card is often a part of the KYC process.

Figure 15: PAN Allotment – Tax Payer Status

Tax Payer Status	PAN Allotment up to 31/03/2019	Percentage
Association of Persons	12,11,226	0.27
Body of Individuals	73,074	0.02
Company	17,41,192	0.39
Firm	44,32,922	0.99
Government	28,205	0.01
Hindu Undivided Family	20,20,148	0.45
Artificial Juridical Person	37,248	0.01
Local Authority	77,193	0.02
Individuals	43,52,48,341	97.65
Trust	8,47,834	0.19
Total	44,57,17,383	100.00

"Taxpayers status " means the status of taxpayers as per PAN database of Income Tax Department.

"Percentage" means percentage of number of PAN allotted for a given status with respect to total number of PAN allotted.

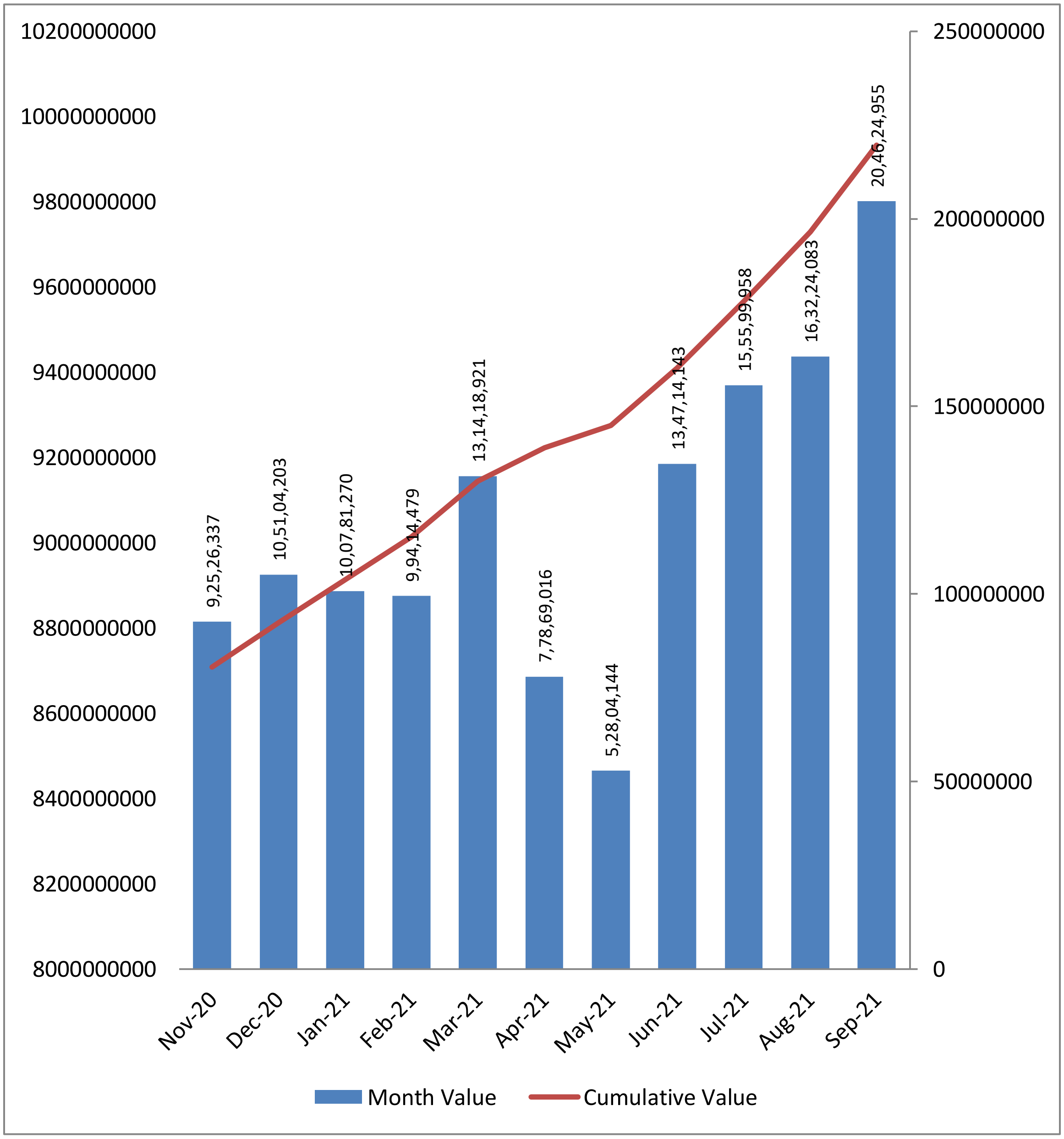
Up to 31.03.2019 total 24,90,68,879 PANs have been linked with the Aadhar.

Source: Incometax.gov.in

e-KYC

UIDAI has initiated Aadhaar Paperless Offline e-KYC verification process for Aadhaar card holders to voluntarily use it for proving their identity in the various applications in paperless and electronic fashion without compromising on privacy, security or inclusion. The Aadhaar Paperless Offline e-KYC service enables instant verification of the user's identity thereby cutting down on the hassle or cost of paper based verification and KYC. The offline e-KYC process eliminates the need for the resident to provide photo copy of the Aadhaar letter and instead can download the KYC XML and share the same with the agencies who seek the required KYC. The entire paperless offline e-KYC process is highly secure. The KYC data is shared directly by the Aadhaar card holder without the knowledge of UIDAI, without the need to reveal the Aadhaar number of the individual. Biometric verification (like fingerprints or iris scan) is also not needed for such verification. The Aadhaar KYC data downloadable by Aadhaar number holder is digitally signed by UIDAI to verify authenticity and detect any tampering. The entire data is encrypted with the clause provided by the Aadhaar number holder allowing residents control of their data.

Figure 16: e-KYC Trend, Nov 2020 – Sep 2021



Source : Uidai.gov.in

Digital Applications

Income Tax Filing

eSignatures are widely used in filing income tax and GST. As per income tax department, there were 8.45 crore individual tax payers in assessment year 2018-19. This is a substantial increase from 5.26 crore in assessment year 2013-14. Online tax filing requires use of eSignature that boosts the demand for the solution. As the GDP of the country improves, GDR per capita would increase and hence would push up the number of tax payers in the country.

Figure 17: Number of Tax payers in India, AY 2013-14 till AY 2018-19

Tay payer Category	AY 2013-14	AY 2014-15	AY 2015-16	AY 2016-17	AY 2017-18	AY 2018-19
AOP	1,41,212	1,59,640	1,80,321	2,05,725	2,25,599	2,56,689
BOI	6,141	6,986	7,433	8,650	9,246	10,418
Company	7,02,828	7,46,800	7,68,206	8,10,617	8,37,597	8,86,889
Firm	10,35,688	10,83,515	11,56,136	12,50,519	13,12,488	14,25,375
Government	183	334	485	747	1,308	2,556
HUF	9,60,004	9,99,401	10,55,205	11,19,899	11,35,677	11,87,180
AJP	10,211	10,556	11,098	11,702	11,506	12,106
Local Authority	5,916	7,118	7,533	8,358	9,096	10,185
Individual	4,95,76,555	5,38,05,146	5,79,70,144	6,55,55,912	7,04,45,510	8,04,45,511
AOP (Trust)	2,05,758	2,17,092	2,31,781	2,53,070	2,61,531	2,84,578
Total	**5,26,44,496**	**5,70,36,588**	**6,13,88,342**	**6,92,25,199**	**7,42,49,558**	**8,45,21,487**

AY: Assessment Year, AOP: Association of Persons, BOI: Body of Individuals, HUF: Hindu Undivided Family, AJP: Artificial Juridical Person

Source: Incometaxindia.gov.in

GST Filing

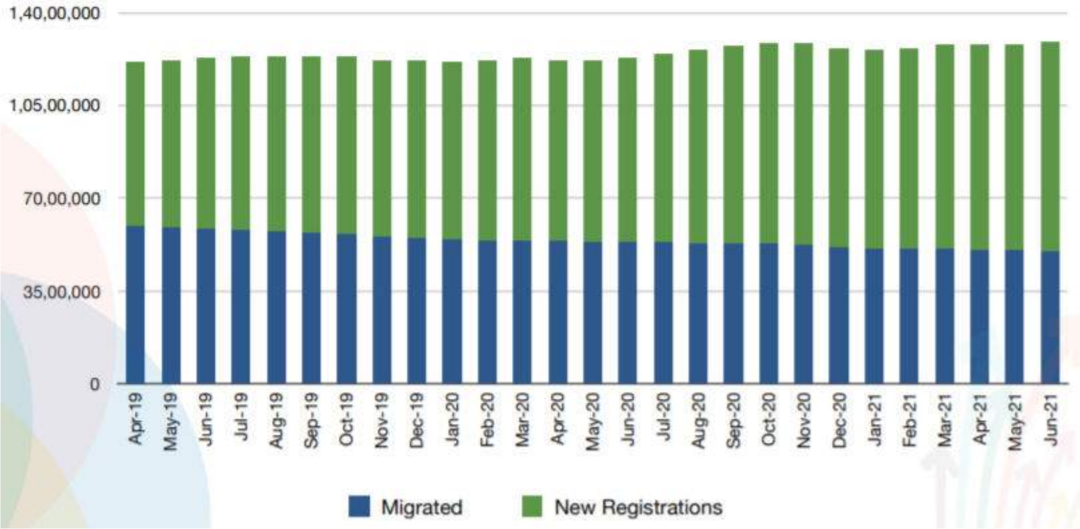
First implemented in July 2017, the Goods and Services (GST) Tax is an indirect tax used in India on the supply of goods and services. It was introduced to replace a number of indirect taxes (like value added tax, service tax, purchase tax, excise duty, etc.). Every buyer (manufacturer, service provider, retailer, and consumer) has to pay GST for every purchase they make. Catogorized into 4 different types: central GST, state GST, integrated GST, and union territory GST; e-commerce aggregators, individuals, agents of input service distributors, non resident individuals who pay tax, and businesses are supposed to pay GST.

Any company (total annual income of INR. 20 lakhs or more) who is eligible under the GST scheme must register in the GST portal developed by the Government of India. It is 15 digit distinctive code that is provided to every taxpayer called the GSTIN. A GST certificate is issued by the authorities in the form of GST REG-06. This is an electronic certificate which contains GSTIN, Legal Name, Trade Name, Constitution of Business, Address, Date of liability, Period of Validity, Types of Registration, Particulars of Approving Authority, Signature, Details of the Approving GST officer, and Date of issue of a certificate. A valid Class 3 digital signature is required for GST registration and filing. According to the norms laid down in GST, all documents submitted including GST registration applications or documents to the portal needs to be digitally signed. This has created the demand for eSignature solutions in the recent past which is expected to increase even further over the period of time.

Number of Registered Persons in GST as on 31st July, 2021

129.92 Lakhs

Figure 18: GST Registration Trend (Active Taxpayers Net of Cancellations), Apr 2019 – Jun 2021

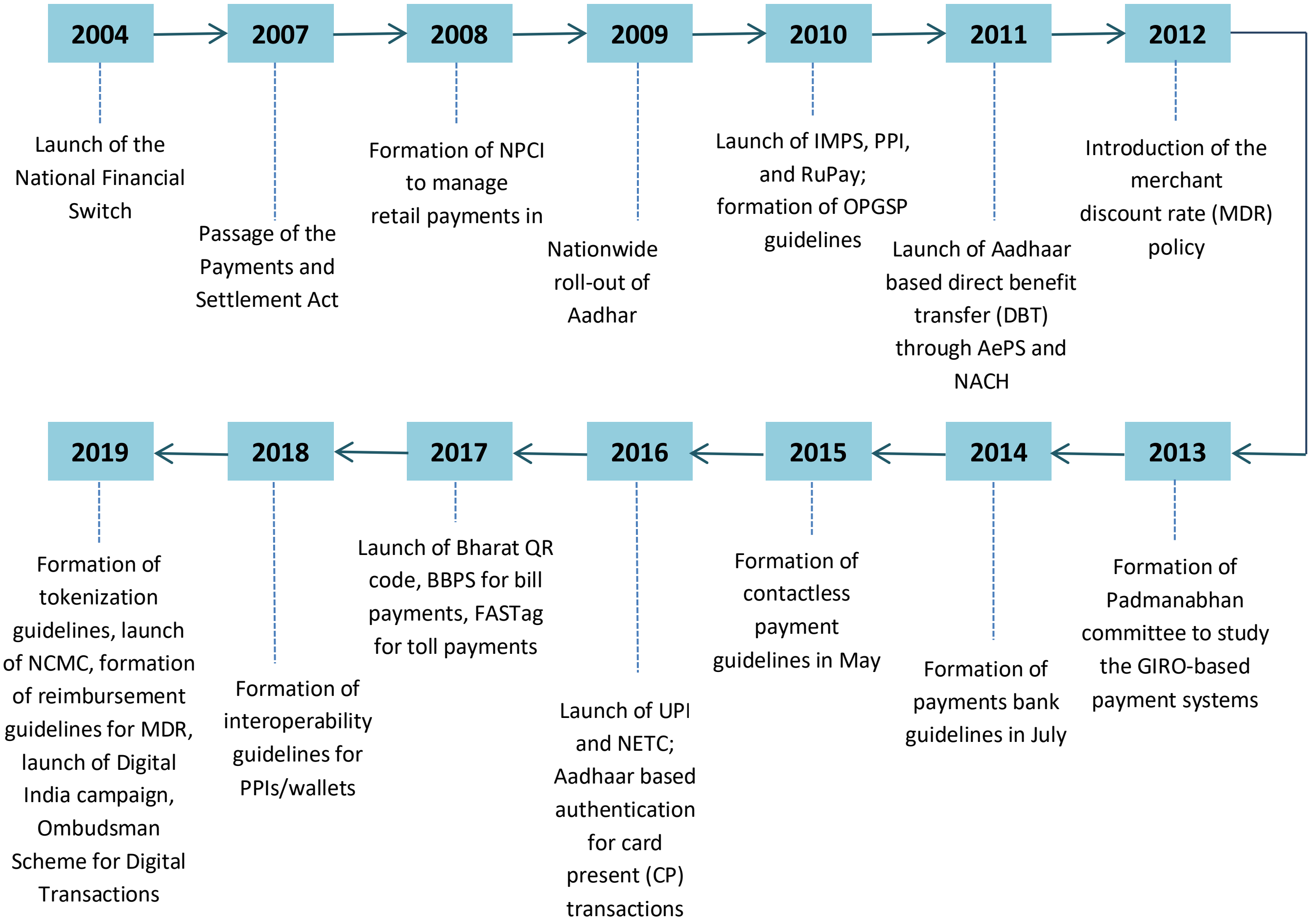


Figures as at the end of the month,
Figures include all kinds of Registration except UIN
Figures are net of cancellation and revocation of cancellation ith retrospective effect
The number of migrated tasxpayers is as per date of liability (not when the migration got completed) which is 1st July 2017, irrespective of date of migration
Source: gst.gov.in

Digital Payments and Transactions

Over the last few years, India has seen a strong growth in the digital payments ecosystem. The country is fast moving from cash to cash-less society. People want convinience and quicker transactions which is being enabled through digital payments. The Reserve Bank of India (RBI) has taken number of steps like adoption of the National Common Mobility Card (NCMC), licences to White Label ATM operators, issuance of Europay, Mastercard and Visa (EMV) and Near Field Communication (NFC) based cards and customer grievance redressal to boost digital payments and improve security.

Figure 19: Key Developments in Digital Payments, India


2004
Launch of the National Financial Switch
2007
Passage of the Payments and Settlement Act
2008
Formation of NPCI to manage retail payments in
2009
Nationwide roll-out of Aadhar
2010
Launch of IMPS, PPI, and RuPay; formation of OPGSP guidelines
2011
Launch of Aadhaar based direct benefit transfer (DBT) through AePS and NACH
2012
Introduction of the merchant discount rate (MDR) policy
2013
Formation of Padmanabhan committee to study the GIRO-based payment systems
2014
Formation of payments bank guidelines in July
2015
Formation of contactless payment guidelines in May
2016
Launch of UPI and NETC; Aadhaar based authentication for card present (CP) transactions
2017
Launch of Bharat QR code, BBPS for bill payments, FASTag for toll payments
2018
Formation of interoperability guidelines for PPIs/wallets
2019
Formation of tokenization guidelines, launch of NCMC, formation of reimbursement guidelines for MDR, launch of Digital India campaign, Ombudsman Scheme for Digital Transactions

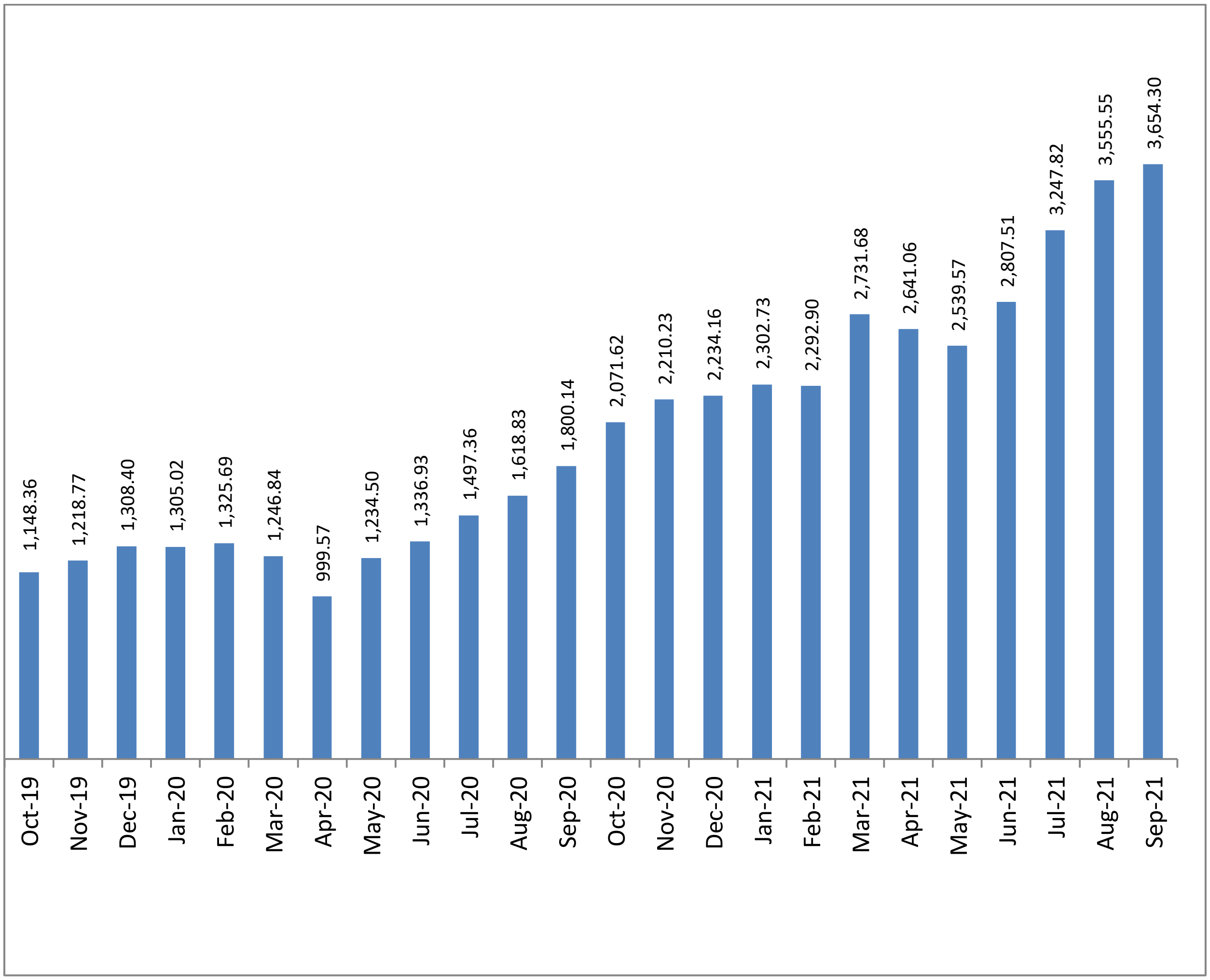
Source: RBI and NPCI

The ongoing COVID-19 pandemic has accelerated the adoption of digital payments. Users have started to avoid cash transactions to minimize the chance of infections. Regular visits to ATMs and banks have reduced as users have shifted towards mobile wallets, UPI payments, NEFTs and IMPS. From doing mobile recharges, grocery shopping to making payments for high value purchases – consumers have started to prefer digital modes of payment; at least in the major cities of the country.

- **UPI**

UPI refers to Unified Payment Interface, initiated by the National Payments Corporation of India (NPCI) in co-ordination with the Reserve Bank of India and Indian Banks Association (IBA). UPI is considered as a major step towards the Government's aim to achieve a cashless economy. Payments are made through smartphones which acts as a virtual debit card. Users can send/receive money instantly without any hassel. In the last 2 years (Oct 2019 to Sept 2021), the number of UPI transactions have increased at a YoY of 101.3%.

Figure 20: UPI Transaction Volumes (in Mn.), Oct 2019 – Sep 2021

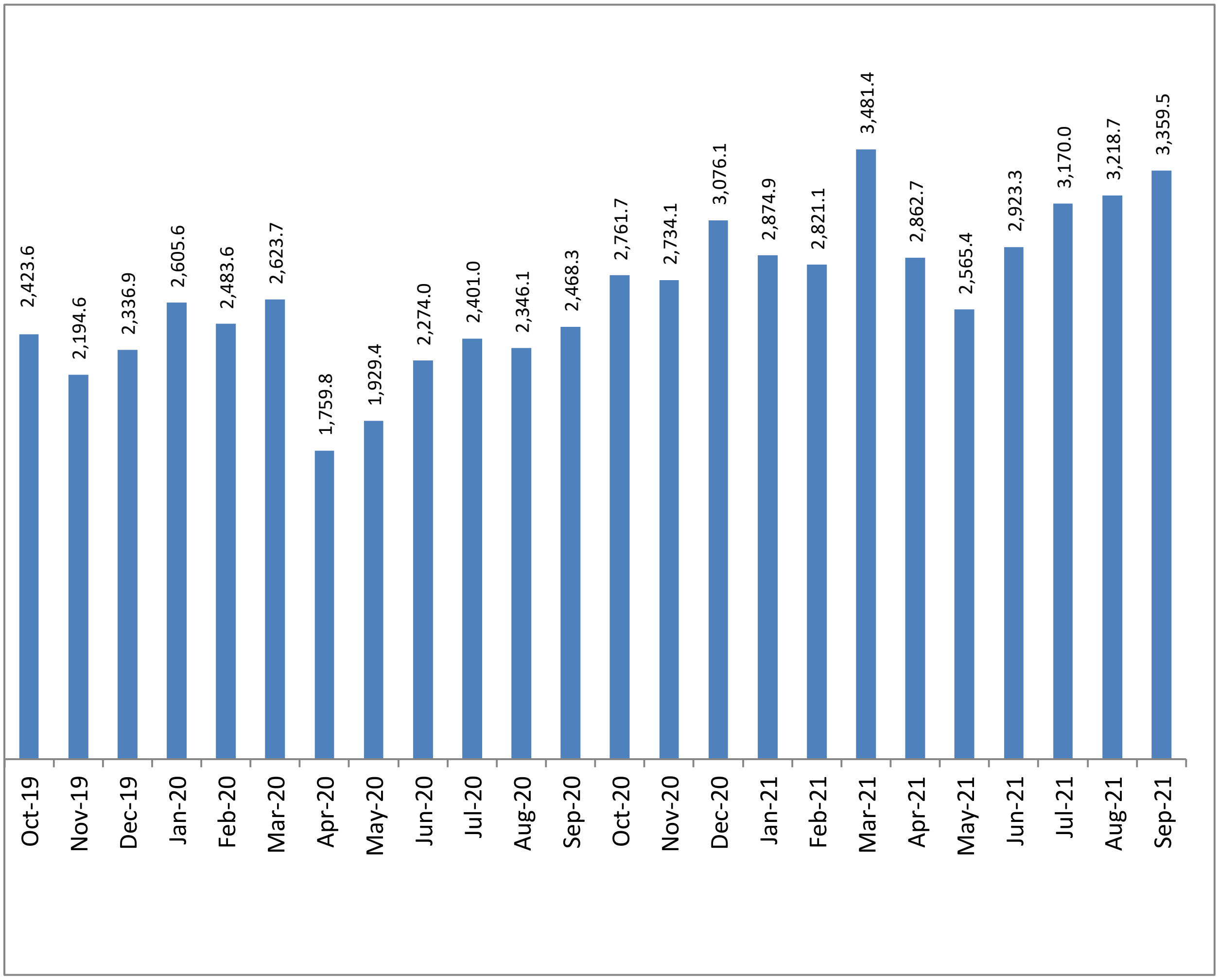


Source: NPCI

- **NEFT**

One of the most common types of digital payment modes that users employ is NEFT (National Electronic Funds Transfer). It quickly transfers money between banks throughout India. Instead of standing in queues for long hours, customers can transfer money as much as INR. 25 lakhs per day via online NEFT. Inward transactions at the recipient bank branch for credit to beneficiary account are free of cost. However, outward transactions at the transaction initiating bank branches are often chargeable.

Figure 21: Number of NEFT Transactions (in Lakhs), Oct 2019 – Sep 2021



Source: RBI

- NACH

The National Automated Clearing House (NACH), developed by NPCI, is a web based solution to facilitate interbank, high volume, electronic transactions which are repetitive and periodic in nature. The NACH system is used by banks,financial institutions, corporates and government for making bulk transactions towards distribution of subsidies, dividends, interest, salary, pension etc. and also for bulk transactions towards collection of payments pertaining to telephone, electricity, water, loans, investments in mutual funds, insurance premium etc.

In 2020, NPCI has reintroduced e-Sign based electronic NACH mandates. The main motive behind the reintroduction was to counter the existing drawbacks of paper based NACH. The original paper based NACH procedure was time consuming and expensive for service providers. NACH authorization requests saw high number of rejections (as much as 30%). This was mostly due to signature mismatch, missing details, soiled forms, etc. Both these spiraled the overall customer acquisition costs and delayed money transfer.

To enable faster processing, NPCI allowed eSign based eNACH. eSign uses Aadhaar based verification. The overall eSign based verification is a simple process which includes:

1. Customers to choose the eNACH through eSign on the service providers website or app
2. The company's website/app makes a server side API call to eSign service provider to create an authentication session for the user
3. Customer verification is done through OTP based authentication sent on his/her mobile number
4. After the authentication is completed, e-Sign solution provider sends the authorized eSigned mandate to the Sponsor Bank in real time
5. The Sponsor bank sends the mandate to NPCI along with the acknowledgement
6. NPCI sends the esigned mandate to the Destination bank which is also the customer's bank
7. Finally, on verification by the destination bank, it sends a confirmation message to the customer

Benefits of eSign based eNACH
• Saves time as eSign based eNACH authorization mandates are processed in real time
• Due to reduced paperwork, there is a cost savings
• Enables faster customer onboarding
• Reduced risk of a fraud
• Legally valid

Figure 22: Volume of Sucessful NACH Transaction, FY 2014 – FY 2021

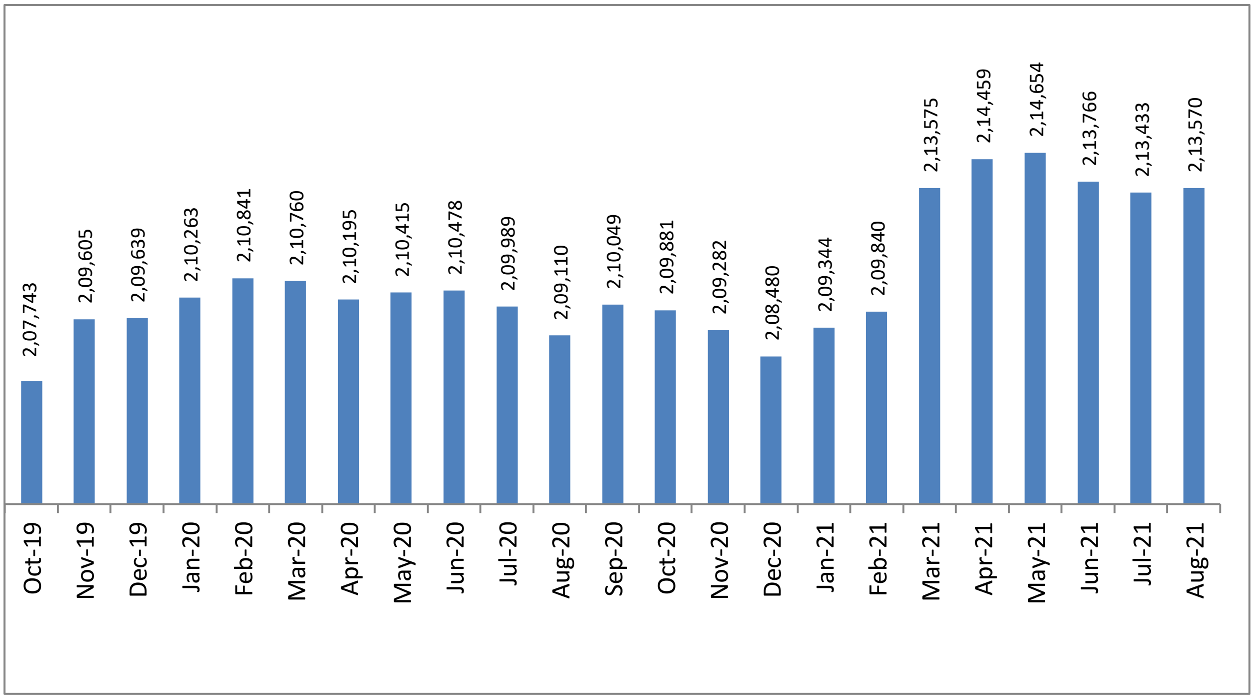
Year	Volume (Nos.) of Sucessful NACH Transactions
FY 2013 – 14	8,49,88,751
FY 2014 – 15	32,65,03,100
FY 2015 – 16	1,39,27,89,308
FY 2016 – 17	1,96,75,20,109
FY 2017 – 18	2,37,49,08,314
FY 2018 – 19	2,86,13,80,436
FY 2019 – 20	3,40,10,34,126
FY 2020 – 21	1,73,02,42,91,938

Source: NPCI

- **ATMs, PoS Machines, Bank Cards**

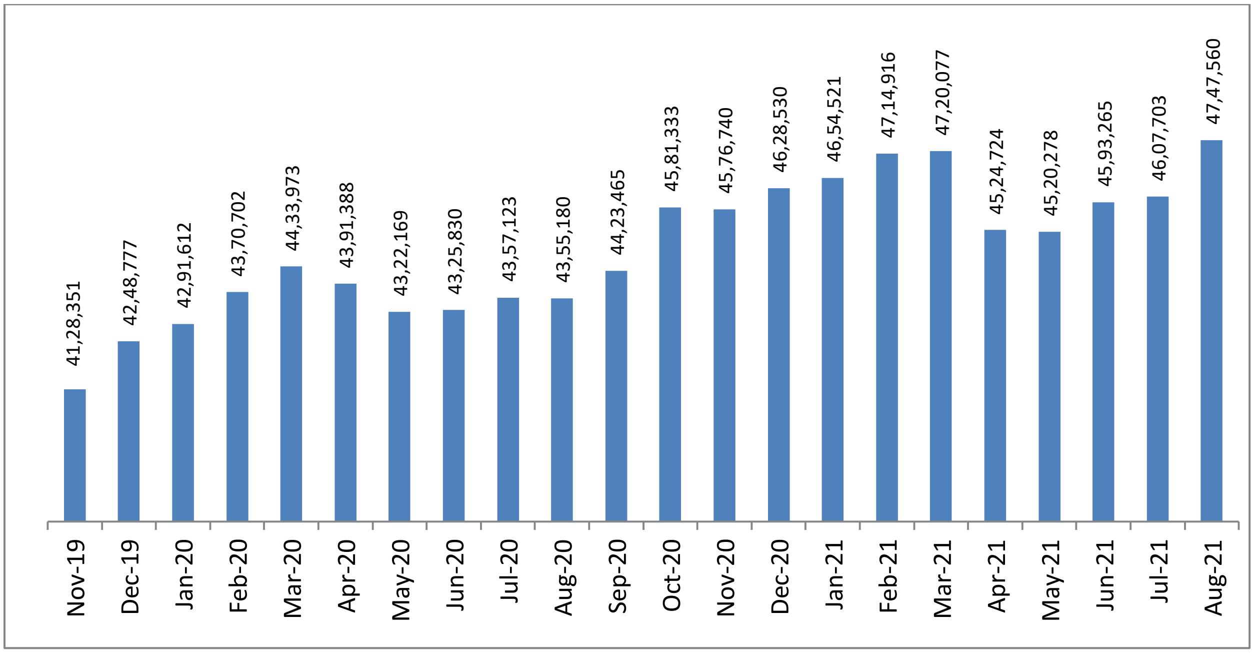
While online banking has taken up pace, the bank cards (debit and credit) market has strong market hold. Instead of visiting banks, customers go to ATM kiosks for withdrawing money. ATMs (debit cards) are primary instruments in such transaction. A steady growth of bank cards noticed in India despite the strong adoption of online banking, mobile wallets and UPI payments. The number of ATM machines in India has also increased over the period as cash transactions continue to hold base. Also, POS (point of sale) machines are common transaction devices across the large and medium stores in India. Oxigen, Verifone, Ingenico, mSwipe, and Paytm are the leading POS providers in India with each machine costs at a range between INR. 3000 to INR. 7000.

Figure 23: Number of ATMs in India, Oct 2019 – Aug 2021



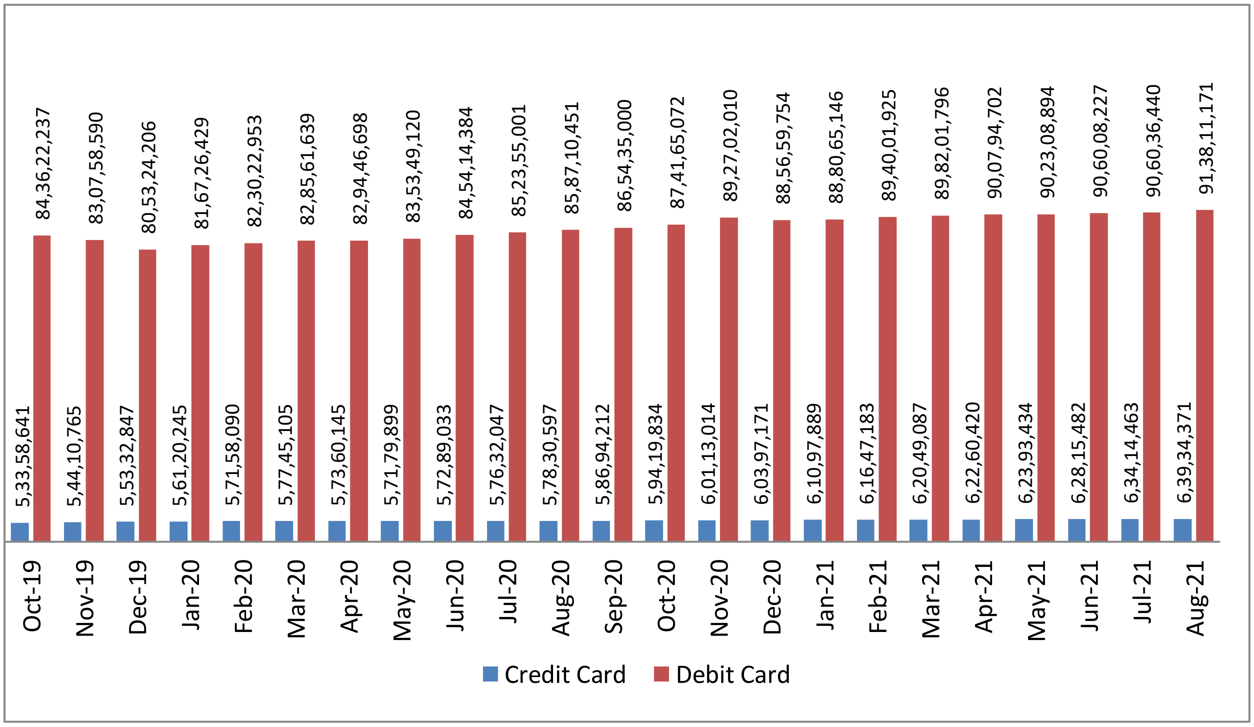
Source: RBI

Figure 24: Number of POS Machines in India, Nov 2019 – Aug 2021



Source: RBI

Figure 25: Number of Credit and Debit Cards in India, Oct 2019 – Aug 2021

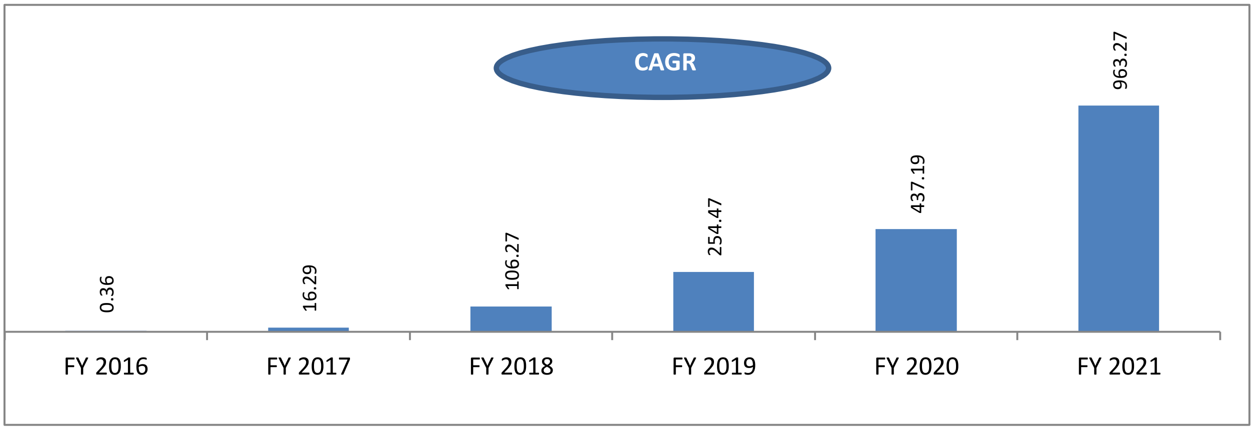


Source: RBI

- **AEPS over Micro ATMs**

NPCI defines AEPS (Aadhaar Enabled Payment System) as a bank led model which allows online interoperable financial inclusion transaction at PoS (MicroATM) through the business correspondent of any bank using the Aadhaar authentication. The objective is to empower a bank customer to use his/her Aadhaar to access his/her respective Aadhaar enabled bank account and perform basic banking transactions like cash deposit, cash withdrawal, Intrabank or interbank fund transfer, balance enquiry and obtain a mini statement through a Business Correspondent.

Figure 26: Number of AEPS Txn. over Micro ATM (Cash Withdrawal/Deposit) (in Mn.), FY 2016 – FY 2021



CAGR from FY 2016 till FY2021

Source: NPCI

1.5. Impact of Cybersecurity on Digital Transformation

While governments are focusing on bringing in and investing on various digital initiatives, cybersecurity remains as the most important aspect within the entire process. For the volumes of data that the government deals with, it is critical that the data is secured at the highest possible manner. As per The World Economic Forum, it is estimated that $1 trillion is lost to financial crimes annually; with fraudsters employing different techniques from phishing scams to identity theft for launching sophisticated attacks. Financial and user data needs to be encrypted with the right authentication technique to prevent these breaches. Users and financial institutions need to abide by KYC norms to prevent any financial fraud or be a prey in money laundering activities. KYC, considered as a strong protection instrument, helps in identifying and verifying the identity of the customer through independent and reliable sources of documents, data or information. Banks use passwords, PIN numbers and other forms of knowledge based identification for securing financial transactions. Password based authentication is not considered the most effective modes, however is the most common identification method.

To step up and provide an improved authentication technique, banks are taking help of MFA (multi factor authentication), biometrics, Aadhaar based authentication and OTP (one time password). MFA is a multi-layered cybersecurity approach to prevent frauds related to identity theft. The approach acts a foundation to protect digital channels and improve customer’s trust towards digital banking by protecting senstive financial and trasactional data, applications, and devices across bank employees and customers. Studies suggest that MFA can prevent ~99% of the attacks that rely on stolen credentials. Advanced authentication techniques provide granular level of security including adaptive and risk based authentication. Digital Signature Certificates are used for authentication of high value fund transfers. With online and electronic transactions growing, digital signature offers added layer of security. Increasing data breach incidents further bolster market growth. 3D facial recognition and iris scan are newer security techniques that banks and other financial institutions are likely to rely on the near future.

2. Growing Impetus on Secured Digital Transformation

2.1. Challenges in Digital Transformation

Digital Transformation (DT) is key in today's context irrespective of the size and nature of the enterprise. Government agencies, banks, financial institutions, private enterprises, education institutions, etc. has started the DT journey to remain competitive and stay ahead in the race. Companies are investing on next generation tehnologies like AI, ML, automation, cloud and analytics to improve operational efficiency, improve productivity and deliver exceptional customer experience. However, what bother enterprises is the concern round cybersecurity.

Most enterprises (private, public or government) have made sure that they have some kind of online presence to improve easy accessibility and visibility. E-commerce and online banking are two of the most common web based services opted by customer. Growing volume of transactions open up vulnerabilities for cyber criminals to exploit. Data hosted on the website could be breached or attackers could fake versions of the site. Identity could be jeopardized; identity theft can become common without the right authentication techniques.

Digital Signature Certificates (DSC) are critical towards embarking a secured digital transformation journey. DSC makes sure that electronic documents have complete protection by ensuring authenticity of the documents. It authenticates the identity of the individual and the business holding the certificate issued by a CA. Signing confidential documents (like contracts, legal documents, lease agreements, etc.) have become easy with the use of DSC.

Key Security Challenges in Digital Transformation:

- Insecure online interface
- Lack of encryption of data
- Insecure client-server communication
- Poor authentication techniques used
- Struggles to adhere to regulations (like PCI/DSS)
- No or outdated digital certificates
- Limited measures on non-repudiation
- No and unsecured paperless transformation workflows
- Limited identity and access management

2.2. Increasing Security Threat Landscape

The security threat landscape has been evolving on a constant basis and cyber attacks increased significantly during the early phase of the COVID-19 pandemic. Ransomware and phishing were the 2 most common type of cyber attacks noticed during the period. Web application attacks became common so as DDoS (distributed denial of service) attacks. Identity theft resulted in data loss. Employees became a source of insider theft and a major area of concern for the government and enterprises. Enterprises were unprepared to move employees to work from home during the nationwide lockdown (across many countries) as criminals took advantage of this to target employees and their devices.

The ENISA Threat Landscape 2020 maps Malware as the #1 cyber security threat in the EU. Increased number of incidents around web based attacks, phishing, web application attacks, identity theft, and ransomware are noticed. Monetisation continues to hold as the biggest motivation for criminals.

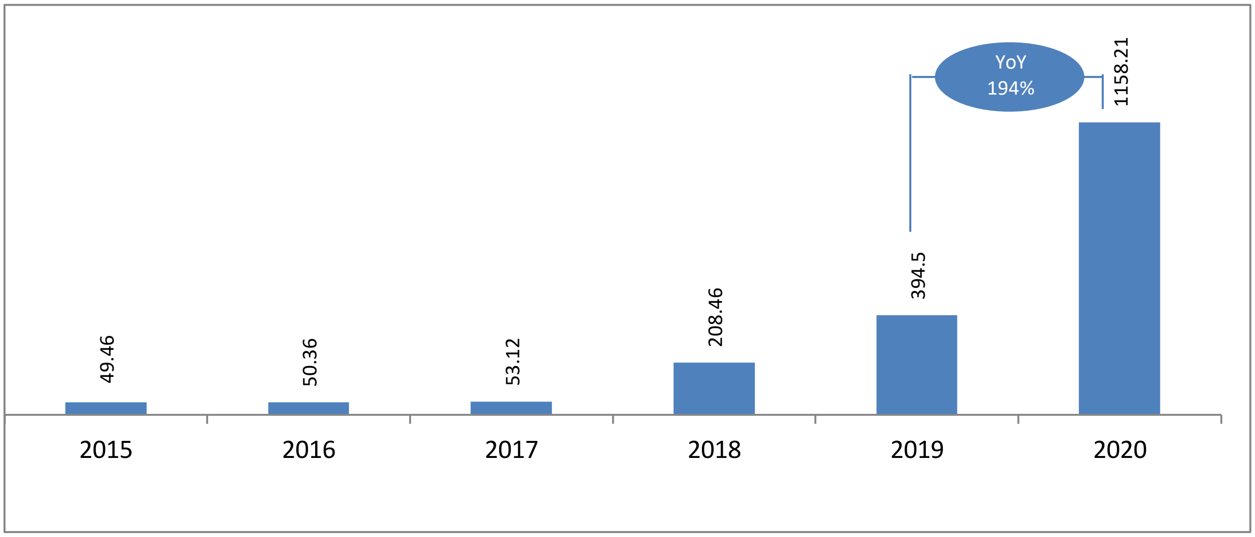
Top 15 Cyber Threats in EU, 2020

1 Malware	2 Web-based attacks	3 Phishing	4 Web Application	5 Spam
6 DDoS Attacks	7 Identity Theft	8 Data Breach	9 Insider Threats	10 Botnets
11 Physical manipulation, amage, theft	12 Information Leakage	13 Ransomware	14 Cyberespionage	15 Cryptojacking

Source: European Union Agency For Cybersecurity (ENISA), 2020

India also noticed a huge jump (194%) in the number of cyber incidents in 2020. As per the CERT-In data, India observed over 6.07 lakh cyber security incidents in the first 6 months of 2021 of which 12,000 incidents were related to the government organizations. Sources of most these attacks are believed to be from countries like Algeria, Brazil, Canada, China, France, Germany, Hong Kong, Indonesia, Netherlands, North Korea, Pakistan, Russia, Serbia, Singapore, South Korea, Sri Lanka, Taiwan, Thailand, Tunisia, Turkey, the U.S., and Vietnam. State sponsored attacks have increased over the course of time which is believed to be the new form of warfare resulting in increased cyber security spending in defence by the government towards guarding strategic interests.

Figure 27: Incidents of cyber attacks across India (in thousands), 2015-2020



Source: MeiTY (India) (CERT-In)

2.3. Enabling Digital Trust, Digital Security and Paperless Transformation

Identity is the foundation of business growth and expansion in the era of digital transformation and represents a ubiquitous security perimeter. The following industry trends are accelerating the need for a modern and comprehensive digital identity platform – IoT Security, Remote Signing and Certificate Discovery.

Digital Trust Service

Digital Trust Services focus on the issuance of digital signature certificates or digital identities to Websites, Individuals, Organizations, or IoT devices in the form of cryptographic key pairs by Certifying Authorities (CAs) or Trust Service Providers who are typically accredited under global standards such as WebTrust and follow the procedures prescribed by such accreditation bodies in issuance of digital signature certificates.

A. SSL/TLS Certificates: In an effort to secure enterprise and customer data, it is critical to create a protective layer of encryption for information transferred between a server and a browser. SSL which stands for Secure Socket Layer makes sure that any information sent to a user's browser or information sent back to the web browser is encrypted. TLS (Transport Layer Security) is just an updated version of SSL. However, SSL is a far more commonly used term and used interchangeably.

SSL/TLS certificates are secured generally with SHA 256 bit hashing algorithm and RSA 2048-bit encryption algorithm. As an alternative to RSA-2048 bit algorithm, ECC (Elliptic Curve) 256 bit algorithm can be used. ECC 256 uses a shorter key length but offers the same level of security as RSA 2048 bit encryption algorithm.

Types of SSL/TLS Certificates

- **Domain Validated (DV) Certificate:** This certificate validates an organization's domain name and domain control. The DV certificate requires little validation and no manual validation steps from the Certifying Authority (CA).
- **Organization Validated (OV) Certificates:** Before a CA issues an OV TLS certificate, the CA must validate the Web site owner's, organizational data, the domain, and the administrator.
- **Extended Validation (EV) Certificates:** The EV TLS certificate requires extensive validation by the CA. Requisites for issuing an EV certificate include verification of an organization's registered legal name, registration number, registered address, physical business address, and any assumed business names. The browser address bar turns green to indicate to the end-users that communication with the Web site is private and the owner of the Web site has been validated.

The above set of certificates can be issued in the following formats

- **Single Domain** allow customers to secure a single domain such as www.domain1.com
- **Wildcard SSL Certificates** allow customers to secure unlimited sub-domains that share the same domain and number of levels. Examples of wildcard domains

include www.company.com, www.domain1.company.com, and www.domain2.company.com.

- **Unified Communications Certificates (UCC)** secures multiple domain names as well as multiple host names within a domain name. For example www.domain1.com, www.domain2.net etc

B. Digital Signature (Individual/Organizational) Certificates

(B.1) Aligned to the Indian market, the Ministry of Corporate Affairs (MCA), Govt. of India, defines Digital Signature Certificate (DSC) as the digital equivalent (that is electronic format) of physical or paper certificates. It is a secure digital key that is issued by the Certifying Authority (CA) for the purpose of validating and certifying the identity of the person holding this certificate. A DSC contains information about the user's name, hash value of the user's identity (for eg. PAN Number), pin code, country, email address, data of issuance of certificate and name of the certifying authority.

- **Who is a Certifying Authority (CA)?**
  In India, a Certifying Authority is an authorized entity licensed by the Controller of Certifying Authorities, under the Ministry of IT, who has the right to issue a DSC. CAs issue millions of certificate every year which is used to protect information, encrypt billions of transactions, and enable secured communication.

Advantages of DSC:

- **Authentication**: DSC helps to authenticate the personal information of a user while transacting/conducting online business.
- **Reduced Cost and Time:** Enables secured paperless transformtion instead of signing hard copies of documents, scanning them and then sending across electronically over email. PDF documents can be signed electronically much quickly with digital signatures.
- **Data Integrity and Authenticity:** Documents that are digitally signed by a user cannot be edited or altered which makes the data safe and secure.
- **Legal Non-repuditation:** Digitally signed documents are considered as legally non-repudiable under the Information Technology Act and action can be taken on the basis of the documents.

Importance of DSC in terms of Compliance:

The importance of DSC has increased considerably as the need to sign documents digitally has increased. The Government of India has put across mandates for individuals and corporates to sign documents electronically there reducing the effort to manage paper documents. Few of the use cases for digital certificates in the Government include:

- Income tax return
- GST
- e-Tendering
- Patent and Trademark e-filing

- IRCTC
- Government eProcurement Marketplace Portal
- Employee Provident Fund Organization
- eOffice
- MCA e-filing
- LLP registration
- Customs e-filing
- e-Bidding
- e-Auction

In addition to the above mentioned, digital signatures are required in different industry verticals like :

- Banking: For customer onboading, lending, etc.
- Enterprise: For enabling fast track paperless office solutions in enterprises
- Government: For accelerating digital transformation in citizen initiatives
- Insurance: For policy generation and streamlined insurance claims
- Mutual Funds and Capital Markets : For easy and seamless customer onboarding and interactions for redemptions, switches

Types of Digital Certificates

Depending on the function, digital certificates can be categoried into 3 different types:

- **Only Sign:** The main purpose of this type of DSC is to sign documents. One of the most common use cases is to sign the PDF file for Tax returns, MCA e-filing and other websites. Signing documents using DSC provides assurance on not only the integrity of the signer but also the data. This is considered as a proof of authentic data (unaltered/tamper free).
- **Only Encrypt:** Encrypt DSC is typically used to encrypt a document and popularly used in the tender portal to help companies encrypt the documents and upload classified information.
- **Sign & Encrypt:** This is meant for both esigning the document as well as encrypting the data before uploading it online. 2 seperate certificates are issued in such cases. It is primarily used to fill government forms and applications.

Class of Certificates

There are 3 class of Digital Signature Certificates issued by the certifying authorities.

- **Class 1 Certificate:** Issued to the individual/private subscribers, the main objective is to confirm the user’s name and email contact details from the clearly defined subject lie within the database of the certifying authority.

  The verification requirements are:

(i) Aadhaar eKYC Biometric or
(ii) Online application form and upload of supporting documents or
(iii) Aadhaar eKYC OTP.
The Private Key generation and storage can be in software.

- **Class 2 Certificate:** Issued to individuals/organizations for the purpose of signing documents.

  The verification requirements are:
  (i) Aadhaar eKYC Biometric or
  (ii) Online application form and upload of supporting documents or
  (iii) Aadhaar eKYC OTP
  (iv) Video Verification

  The Private Key generation and storage should be in Hardware cryptographic device validated to, FIPS 140-2 level 2.

- **Class 3 Certificate:** This class of certificate offers a higher level of assurance and issued to individuals/organizations. It is currently mandated by CCA for all applications effective 1st January, 2021.

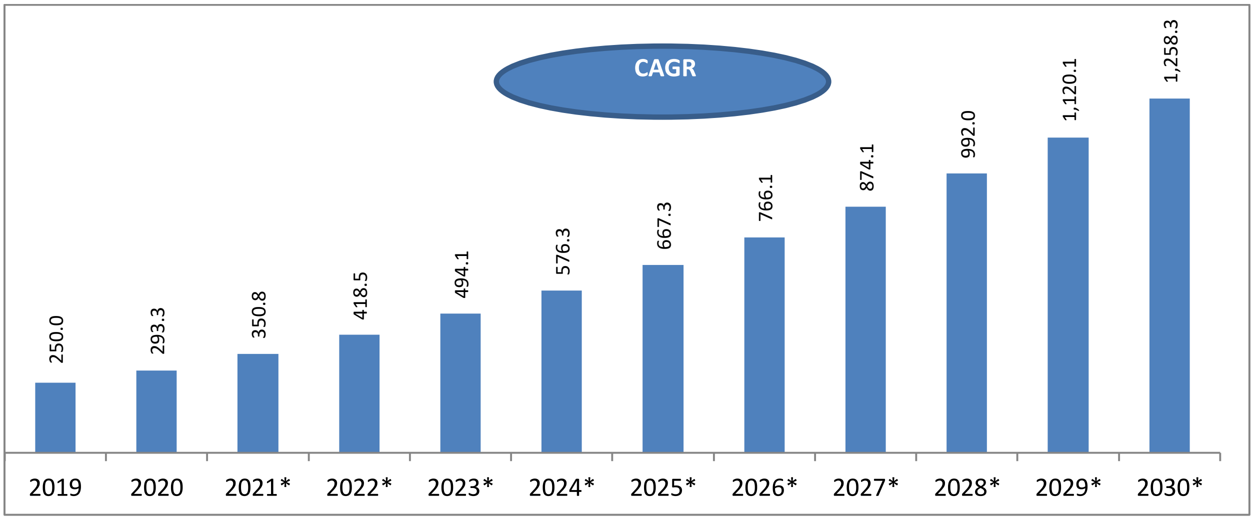
  The verification requirements are:
  (i) Aadhaar eKYC Biometric or
  (ii) Online application form and upload of supporting documents
  (iii) Aadhaar eKYC OTP
  (iv)Video Verification
  The Private Key generation and storage should be in hard ware cryptographic device validated to FIPS 140-2 level 2.

(B.2) Digital certificates also include Code Signing, Encryption, Secure Email Certificate, Post Quantum Certificates, Verified Mark Certificates, Client Certificates, etc.

C. IoT Device Certificates

The huge growth of IoT devices has opened up the opportunity for cyber criminals to exploit the vulnerabilities. The immediate need is to make sure that the IoT devices are secured with the best possible security measures. Unauthorized IoT devices are often seen to be attached to a network without the knowledge and visibility of the security administrator. IoT device certificates are the mechanisms to identify a legitimate device and grant the device access to the network. Without the right authorization of the IT/security admin, no IoT device could be synced in with the network. Authorized devices need device certificates to act as a network passport. Without the right digital certificate, the device would be unable to connect to the network or perform the designated function. IoT devices work in tandem with other security mechanisms to give network access, like device management software applications, mobile device managers or third-party certificate managers.

Figure 28: Number of IoT Connected Devices in India (in Mn.), 2019 to 2030



*Projected, CAGR from 2020 till 2030

Source : Frost & Sullivan

Digital Security Solutions

- **Identity and Access Management (IAM)**

  Most enterprises have started to empower their employees with digitalization; with digital entitlement, the aspect of digital identity has come. Managing the digital identity of employees across different ranks and functions is a challenge that the enterprise IT team has to deal with on a regular basis. This includes on-boarding of new users, creating login credentials, providing privileged access to selected few, lifecycle management, and ensuring identity/governance. From a technology perspective, concepts such as cloud computing, BYOD (bring your own device), and enterprise mobility have increased the need to have improved data security. The amount of data that is stored or transmitted from the cloud needs user restrictions. User and access restrictions should not be only restricted to data security but also to network connections, Web site access, printer access, application access, and more.

  Identity and access management (IAM) is defined as the solution that helps enterprises to determine and control access to application, system and network by end users. It is a set of complementary technologies and methodologies that facilitates identity management, policy controls, access management, authentication, and analytics. With the consumerization of various technologies and business concepts, the need of IAM has increased multifolds.

  Complementary Technologies included in IAM

  - **Identity Management:** Digital identity is a unique identifier assigned to users in cyberspace. The user can be an individual, an organization, or a device. The digital identity is linked to multiple sub-identifiers such as email account, social login, department, etc.
  - **Access Management:** The granting of authorization to use certain services, systems, accounts, or networks based on privilege.

- **Single Sign-on:** An authentication process for users to access multiple applications, systems, or networks using a single set of credentials. SSO increases productivity by eliminating the need to sign in to each individual system or application.
- **Multifactor Authentication:** A requirement to provide two or more independent sources of identification credentials before gaining authorization. This source, or factor, is something a user knows (password) and has (a token or fingerprint).

Other Authentication Modes used in Digital Security/IAM

- **SMS OTP:** This is one of the most common type of authentication techniques used. A one time password (OTP) is sent to the user's registered mobile number which the user types in to authenticate a transaction.
- **TOTP:** Time based OTPs change after a set period of time (60 seconds for example). In India, the mAadhaar app on the mobile phone allows to generate the dynamic OTP instead of waiting for OTP to arrive. The app generates 8 digit dynamic OTP which remains valid for 30 seconds.
- **QR Code:** A Quick Response (QR) Code is a type of matrix type barcode which is scanned using a smartphone. QR codes are widely used in retail where products in supply chain are tracked.
- **Digital Signature Certificates:** Digital Signature Certificates allow the user to authenticate themselves to online applications using assymetric cryptographic key pairs.
- **Knowledge based Authentication:** Known as KBA, it is one of the authentication techniques where the user is required to answer at least one 'secret' question. KBA is often used as part of MFA or while retrieving a password.
- **Grid Authentication:** This is a type of authentication where the user enters value from specific cells into a grid whose content should be only accessible to him and the service provider. This method of authentication is also known as bingo card authentication since the letters and numbers are typed in the grid in rows and columns.
- **Smart card Authentication:** Common in an enterprise setup, users are provided access who has the physical access card. The card is either swipped or placed in front of a smart card reader to grand access.
- **Token Authentication:** It is an authentication technique that allows users to verify their identity before they receive a unique access token. The user retains access as long as the token provided to him/her remains valid.
- **Adaptive Authentication:** Also known as risk based or contextual authentication, this is an advanced authentication technique where the profile of the user is created and depending on the situation (geographic location, device, or insecured network), the authentication technique changes accordingly.
- **Biometric:** Uses biometrics like fingerprints or retina scans to identify a person.
- **FIDO U2F:** Known as FIDO Universal Second Factor (U2F) athentication, it allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. After the user logs in using the username and

password, the service prompts the user to present a second factor device (such as a FIDO Security Key) at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4–digit PIN) without compromising security.

- **Public Key Infrastructure (PKI)**
  PKI is the basic platform for issuing digital certificates using assymetric key pair based encryption and binding them to users, websites or devices. The certificates help identify the user and authenticate the transaction originated by the user in a manner so as to ensure data integrity and authenticity. Issuance of certificates such as SSL/TLS certificates and Digital Certificates use as a platform for issuing, reissuing and revoking certificates as well for managing identity lifecycle.

  PKI is defined as an infrastructure consisting of necessary systems and applications to manage the issuance and lifecycle of digital certificates. PKI system consists of the following key components: CA (Certificate Authority) for issuance of certificates, RA (Registration Authority) to verify user identity, a CRL/OCSP (certificate revocation list/online certificate status protocol) to publish revocation status of certificates, and a timestamping system to provide timestamping service. Implementing a PKI system in an organization solves many security issues while enhancing its ability to adopt presenceless, paperless and cashless way of doing business and enhancing customer experience. There are many incentives for implementing a PKI solution in an organization, the major four are:
  - Identity management and authentication, both logical and physical authentication
  - Digital signing for reducing paper work, saving time in signature rounds and non-repudiation
  - Encrypting data to prevent data leakage
  - Compliance with government regulations

Paperless Transformation and eSignature Workflow Solutions

Enterprises are fast moving towards paperless offices bur are still stuck with the last mile hurdle of paper which requires signature. eSignature Workflow solutions are able to solve this last mile problem by allowing end users to digitally sign documents that are legally valid and compliant. Thus eSignature workflow solutions enable organizations to transform fully to paperless offices as opposed to scanning solutions. Going paperless helps improve customer experience, convenience, compliance and reduce cost. It enables paperless and presenceless transactions and is considered eco-friendly. Paperless process help improve flexibility, quicker turnarounds, and better managebility without compromising on security. However, to embark the paperless transformation journey, it is critical that enterprises choose the right solution. Processes need to be designed well or could end up in inefficiencies.

Important features that a Paperless Transformation Solution should have:

- Supports eSignature
- Caters to the fast changing business requirements
- Leverages the best in class technologies to improve performance
- Available as on-premise and cloud deployments

- Adheres to global and local industry regulations and mandates
- Integrates with other 3rd party applications like ERP and CRM
- Offers the best in class security

2.4. Role of Automation, Artificial Intelligence and Cloud in Digital Security and Paperless Transformation

To stay ahead in the Digital Transformation journey, it is important for enterprises to invest on next generation technologies. Enterprises need to leverage next generation technologies to improve the efficiency of digital trust and security solutions and enable paperless transformation.

- **Automation in Digital Certificate Management**

  There is an utmost need to automate digital trust specifically certificate management. Automation in digital certificate management helps save time and money by reducing manual efforts. Chances of error also reduce considerably thereby improving operational efficiency. Automation helps reduce repetitive and time consuming manual tasks. High volume of certificate creation and validation can be achieved through automation. Updates and audit sensitive processes can be streamlined using automation.

  Certificate management tasks that can be eased with the help of automation:

  - Auto renewal of digital certificates through certificate discovery
  - Digital certificate validation
  - Automate alerts for various tasks
  - Report generation
  - Enable visibility on potential risks and vulnerabilities with greater visibility over the organization’s entire certificate landscape
  - Revocation of certificates
  - Easy integration with other 3rd party platforms
  - Automated code signing

- **Artificial Intelligence in Paperless Transformation**

  Paperless office based on eSignature orkflow capabilities is likely to be the future. The obvious scene of piled cabinets would soon be gone as it would be replaced with intelligent data management which is easy to manage. Artificial intelligence (AI) and machine learning (ML) would be the most important technologies behind the transformation.

  AI would help in efficient documentation. Employees would save time in searching documents, information would be readily available. Restricting confidential information would be much easy. Paperless offices would require lesser storage space and volumes (terabytes) of data could be stored. When it comes to signature, AI would empower electronic signing to transform customer experience and help manage risk governance.

- **The availability of Cloud based Solutions**

In the last few years, vendors have started to come up with cloud based solutions. Unlike on-premise products, cloud based solutions are easy to deploy and are often budget friendly. Product updates come in automatically and can be installed on one's wish. However, some of the regulated industry verticals like banking prefer the use of on-premise or private cloud solutions where they have direct control over the data and its security.

2.5. Growth Drivers to Digital Trust, Digital Security, and Paperless Transformation

Digital Trust Services

SSL/TLS Certificates

- The need to secure user data, verify ownership of websites, prevent attackers from creating fake version of sites and build trustworthiness among users.
- To improve search engine ranking
- To adhere to regulatory standards and mandates

Digital Signature Certificates

- Establish user identification and authentication
- Maintain confidentiality and integrity of the message or transaction
- Legal non-repudiation
- Enable paperless transformation

IoT Certificates

- Establish proof of identity for the IoT device
- Encryption of data
- Data integrity
- Better lifecycle management

Digital Security Solutions

Identity and Access Management

- Growing importance of IAM in digital transformation
- Relevance of IAM in cloud environment
- Leverage the power of automation (RPA) in IAM solutions and simplify security processes
- Industry regulations and mandates

Public Key Infrastructure (PKI)

- Government initiatives and regulations that involve PKI technology
- Embedding PKI on various devices (eg. mobile phones)
- Non-repudiation services that relay on PKI solutions
- Acceptance of the PKI as a non-problematic solution
- Cost reduction of the PKI solution for SMBs

Paperless Transformation Solutions

- Aim to become a digital first company

- Deal with the challenge of space in offices
- Save money in printing documents, become environment friendly (decrease carbon footprint)
- Boost productivity and improve efficiency
- Improve security of data stored
- Make documentation and secured data sharing
- Automatic data retention and digital backups
- Adhere to audit guidelines

2.6. Digital Initiatives across Key Industry Verticals

Government and Public

- **DigiDhan Abhiyaan**

  With an aim to promote digital payments and become a less cash economy, the Government of India has launched the DigiDhan Abhiyan. This is an initiative by the Ministry of Electronics and IT. The initiative enables Indian citizen, small trader and merchant to promote digital payment in their everyday transactions. As per MeiTY data, there were :

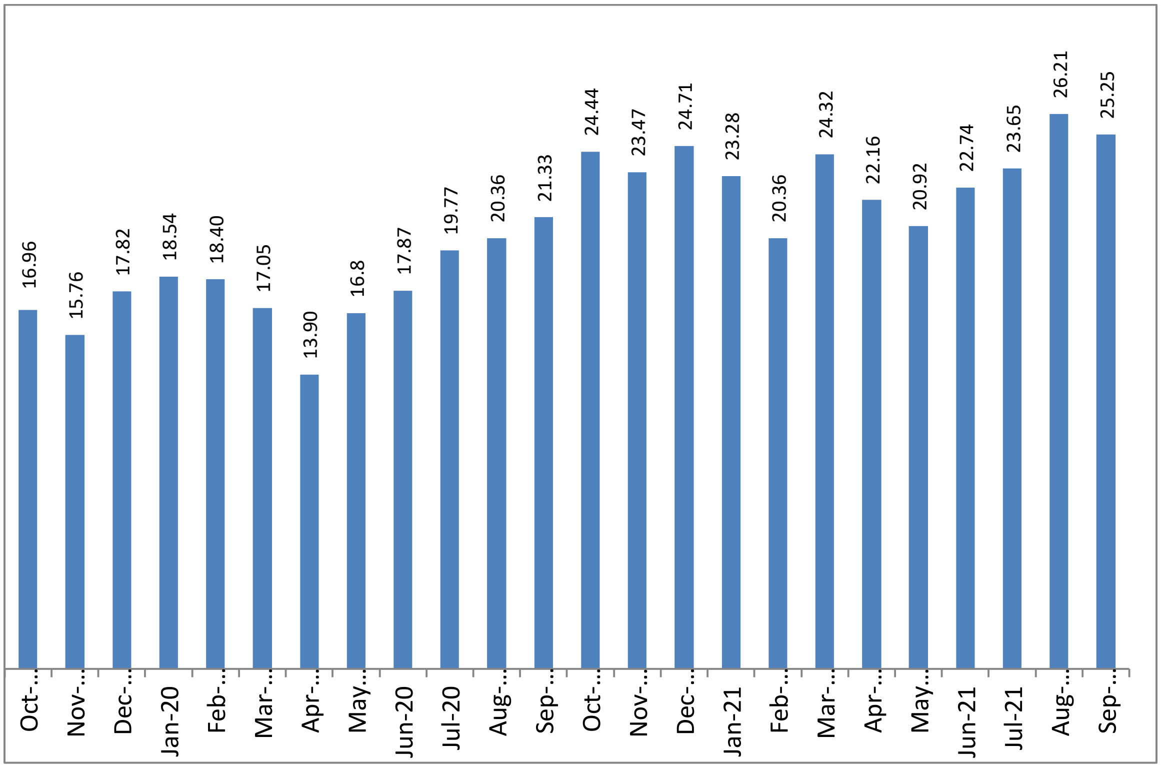
  - 4572 Crore digital transactions for 2019-20
  - 57,87,878 Physical & Mobile POS deployed till 26/06/2020
  - 11,27,799 BHIM Aadhaar Pay POS deployed till 26/06/2020

  The DigiDhan Abhiyaan has launched a free to air channel called DigiShala to impart information in rural and semi urban areas on digital payment ecosystem. The channel educates people (aimed at rural India) to make digital payments using UPI, USSD, Aadhar enabled payment systems (AEPS), e-wallets, cards etc. AEPS uses Aadhaar Authentication for user identity and authentication.

- **BHIM (Bharat Interface For Money) Aadhaar Pay**

  BHIM is India’s mobile payment app developed by the National Payments Corporation of India (NPCI) which is used to facilitate e-payments directly through the bank and encourages cashless transactions. BHIM Aadhaar Pay enable merchants to receive digital payments from customers over the counter through Aadhaar Authentication. It allows any Merchant associated with any acquiring bank live on BHIM Aadhaar Pay, to accept payment from customer of any bank by authenticating customer’s biometrics.

Figure 29: Number of transactions done through BHIM in India, Oct 2019 – Sep 2021



Source : NPCI

- **Digital AIIMS**

  Launched in January 2015, the Digital AIIMS project is part of the Digital India Initiative and is considered for the digital revolution in healthcare in India. This initiative is a linkage between AIIMS, UIDAI and the MeiTY. Using Aadhaar, a unique health identification number for each patient visiting AIIMS is created. This created a digital identity for each patient of the hospital.

  Other Government of India digital initiatives undertaken that require digital identity (primarily Aadhaar):

  - Pradhan Mantri Ujjwala Yojana
  - PAHAL for LPG
  - MGNREGA
  - Electoral Rolls
  - Employees Provident Fund Organization
  - Indira Gandhi National Disability Pension Scheme
  - Indira Gandhi National Old Age Pension Scheme
  - Indira Gandhi National Widow Pension Scheme
  - Mahatma Gandhi National Rural Employment Guarantee Scheme
  - Pradhan Mantri Awas Yojna (Grameen)
  - Prime Minister Scholarship Scheme
  - Education Schemes
  - Cash Transfer of Food Subsidy, etc.

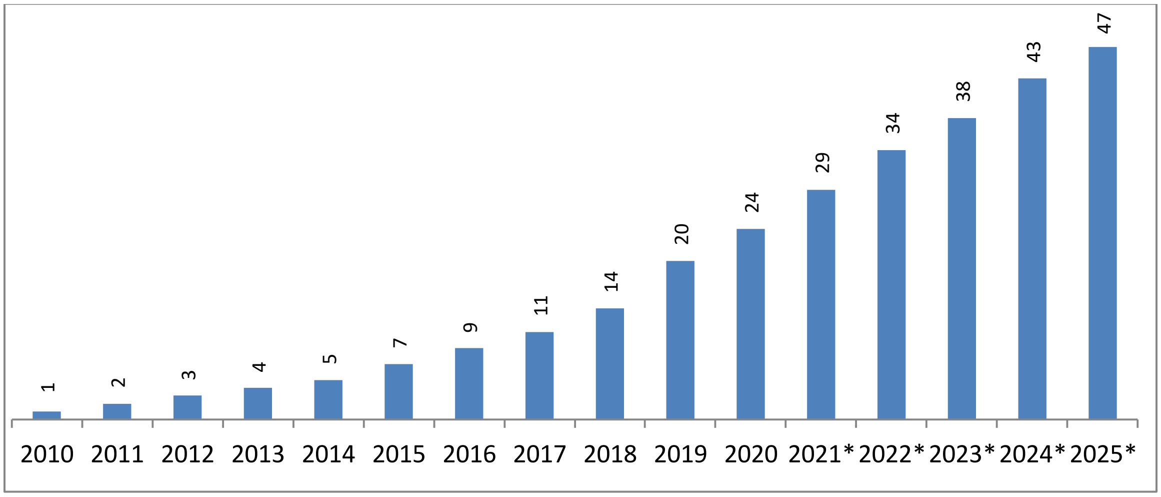
Banking, Financial Services and Insurance

- **Digital Banking**
  The banking industry is fast moving through a phase of aggressive transformation. From loan approvals, and account opening to investments; digital revolution has taken up pace due to the provision around electronic signatures. The adoption of eSignatures in banking processes has proven to deliver significant and quantifiable results in terms of cost reduction, process efficiency, speed of transaction or improved customer experience. The Government of India has been working relentlessly to enable transaction using Aadhaar. Instead of downloading forms, taking print outs, physically signing documents and then uploading onto the websites, customers can quickly generate a document and eSign before passing it on to the bank employees. Application progress status can also be tracked after a document is digitally signed. Mobile apps have even accelerated the use of digital signatures. Customer can not only sign contracts with eSignatures but also renew existing bank deposits.

Use-cases of eSignatures in BFSI :

Banking	Insurance
Customer Onboarding	ePolicy
eStatements	Fraud Mitigation
Electronic Loan Processing	eReceipts
eNACH	eClaims
Trade and Supply Chain Finance	

Figure 30: Online Banking Penetration in India (%), 2010 – 2025



*Projected
Source : Statista

Education

As education becomes global, universities cross home boundaries to open campuses in different countries and locations. Students participate in curriculums as they enrol in global programs. Virtual courses and certifications have gained strong acceptance among students where the need to physically travel to far off campuses have reduced.

eSignature soutions have seen positive response from universities to quickly onboard students, exchange documents with digital signatures, QR codes and timestamp between students and the schools. Students can register to university programs online in real time with the ability to authenticate student identity instantly. Documents can be easily uploaded/downloaded from websites with user identity details captured at the back end. Documents can be indexed, searched and retreived easily without the user being able to alter the date or time of the signature.

Few of the digital use-cases in education include:

- Student registration
- Student onboarding
- Document signing
- Document uploading/downloading
- Issuing of e-certificates to avoid certificate fraud
- Transcript signing
- Faculty contracts
- Fee receipts

Manufacturing

The manufacturing industry has a long value chain. From suppliers to distributers, everyone is part of the manufacturing setup. Every stakeholder is geographically distributed and travelling to the manufacturer’s place is always not feasible. Digital solutions help to share documents among stakeholders from anywhere, anytime and through any device by attaching the valid electronic signatures. Contract documents can be electronically signed, encrypted and sent to recipients by guaranteeing the authenticity, integrity and confidentiality of the document.

Few of the digital use-cases in education include:

- Vendor and Supplier Onboarding
- Easy document sharing among stakeholders
- Data management
- eInvoice and Purchase Order Signing
- Intrgration with 3rd party applications

3. Regulation and Compliance Leading to Digital Security and Paperless Transformation

The global regulatory landscape around digital trust, digital security and paperless transformation is driven by eSignature legislation derived from UNCITRAL Model Law on Electronic Signatures (2001), data privacy acts and sectoral guidelines around cyber security adoption.

3.1. Global

Europe

- **General Data Protection Regulation (GDPR)**

Popularly known as GDPR, the regulation is an EU law on data protection and privacy in the EU and the European Economic Area (EEA). The main aim of GDPR is to enhance individuals' control and rights over their personal data and to simplify the regulatory enviroment for international business. Following are the different types of privacy data that GDPR protects:

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

While all of the EU countries need to adhere to GDPR, it finally translates to companies that stores or processes personal information about EU citizens even though the company does not have a presence in the EU. Companies who need to comply with GDPR include :

- Located in a EU country
- No presence in EU, but processes personal data of European residents.
- With more than 250 employees
- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data.

- **The eIDAS Regulation**

eIDAS which stands for electronic Identification, Authentication and Trust Services is an EU (European Union) regulation that was estalblished in 2014 and deals with electronic identification and trust services for electronic transactions in EU. The regulation controls use of electronic signatures, electronic transactions, involved bodies, and making sure that online business can be conducted securely. eIDAS has created standards (with similar legal standing as performed on paper) for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enabling electronic transactions.

eIDAS is important in today's context because it eliminates the need for customers to be present physically on-premise like bank to open an account. The regulation is typically beneficial for regulated industry verticals like BFSI and telecom that has the provision to onboard/acquire customers online from anywhere-anytime through the use of electronic signatures.

The United States of America

- **The Electronic Signatures in Global and National Commerce [ESIGN] Act**

Enacted in June 2000, the Electronic Signatures in Global and National Commerce [ESIGN] Act is a US federal law passed by the US Congress to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically. Also known as ESIGN, the act makes sure that there is validity as well as legal effects within contracts that parties electronically enter into. The Act works as a guide on how eSignature service providers serve consumers and how consumers can protect themselves by understanding their rights. While every state in USA has at least a law that pertains to esignature, ESIGN lays down the guidelines governing interstate commerce

- **21 Code of Federal Regulations (CFR) Part 11, the U.S. Food and Drug Administration's (FDA's) regulations for electronic documentation and electronic signatures**

Part 11 of Title 21 of the Code of Federal Regulations (CFR) states how electronic records and signatures are considered trustworthy by the US Food and Drug Administration (FDA). Pertaining to this, the e-signature vendor should be able to meet the technical requirements for achieving Title 21 CFR Part 11 compliance through native product features.

Canada

- **The Personal Information Protection and Electronic Documents Act [PIPEDA]**

Known as PIPEDA, it is a Canadian law that deals with data privacy. It ensures that organizations collect, use and disclose personal information in a manner consistent with the Act (similar to GDPR in Europe). It also allows the creation of electronic alternatives for doing business with government agencies, facilitating the use of electronic documents in judicial proceedings and giving legal recognition to electronic versions of official Parliamentary publications. The Part 2 of the Act describes the characteristics of secure electronic signatures and grant authorities to make regulations prescribing technologies or processes for the purpose of the definition "secure electronic signature".

Before a technology or process can be prescribed:

- the electronic signature must be unique to the person using it
- the person whose electronic signature is on the document must have control of the use of the technology to attach the signature
- the technology must be used to identify the person using the electronic signature
- the electronic signature must be linked to an electronic document to determine if the document has been changed after the electronic signature was attached to it

3.2. India

The relevant laws, rules and regulations surrounding the use of electronic signatures in India include :

- The Information Technology Act (ITA), 2000
- The Indian Contract Act (ICA) of 1872
- The Indian Evidence Act 1872
- The Indian Stamp Act (ISA) of 1899

These laws collectively form the basis and answer the following questions:

- What are the official electronic signatures in India?
- What documents or transactions are not permissible electronically?
- What conditions all contracts must meet, including contracts using an electronic signature that does not meet the officially recognized requirements under the ITA?
- Whether stamp duty needs to be paid for transactions entered electronically?

- **The Information Technology Act, 2000**

  Also known as ITA-2000, the Informafation Technology Act is an Act of the Indian Parliament notified on 17th October 2000 which deals with cybercrime and electronic commerce. Electronic and certificate based digital signatures are regulated by the Act and the following rules were as per the Act:

  - Information Technology (Certifying Authorities) Rules, 2000
  - Digital Signature (End Entity) Rules, 2015
  - Information Technology (Use of Electronic Records and Digital Signature) Rules, 2004

  The IT Act differentiates between electronic signatures and certificate based digital signatures, however both have the same status as that if handwritten signatures. Digital signature is one of the types within electronic signatures which uses an asymmetric crypto system and hash function and uniquely identify the user based on verification guidelines published by the Controller of Certifying Authorities which establishes legal non-repudiation.

  Valid electronic signatures should have an electronic authentication technique specified in the Second Schedule of the IT Act. The Second schedule specifies the following eKYC authentication technique and procedure:

  - Aadhaar eKYC
  - eKYC using PAN

  Following are the criteria for considering an electronic signature reliable and valid:

  - The electronic signature must be unique to the signatory
  - While signing, the signatory must have control over the data used to generate the electronic signature
  - Any change to the affixed electronic signature, or to the document to which the signature is affixed, must be detectable
  - An audit trail of steps is mandatory during the signing process

- The digital signature certificate must be issued by a licensed CA

- **The Indian Contract Act of 1872**

  According to ITA 2000, a contract cannot be denied enforceability only because it was conducted electronically; however the contract needs to fulfill the essential elements of a valid contract as stated under the Indian Contract Act (ICA) of 1872.

  The important points that a valid contract should adhere to as mentioned in Section 10 of ICA include:

  - The contract is entered into by parties who are competent to contract
  - The contract is entered into by parties as a result of their free will (i.e. valid proposal and acceptance)
  - The contract provides mutual consideration between the parties
  - The contract prevents doing of any act which is forbidden by law

- **The Indian Evidence Act, 1872**

  In order to bring in consonance with the electronic methods of execution of documents introduced by the aforementioned IT Act 2000, the Indian Evidence Act 1872 was amended. A particular Section of the Act (Section 65A) recognizes admissibility of electronic records as evidence. According to the Section 65A of the Act, the contents of electronic records may be proved in accordance with the provisions of Section 65B of the Indian Evidence Act.

  Section 65B of the Act states that electronic evidence stored in an electronic mode can be printed on paper, stored, recorded or copied in optical or magnetic media shall be considered and would be admissible in court proceedings. A certificate needs to be presented that recognizes the electronic record having the statement and explicates the way in which it is to be presented.

  Section 73A of the Indian Evidence Act mentions that in order to ascertain whether a digital signature is that of the person by whom it purports to have been fixed, the court can ask the person to apply the public key issued under the CCA Root listed in the Digital Signature Certificate to verify the digital signature purported to have been affixed by that person.

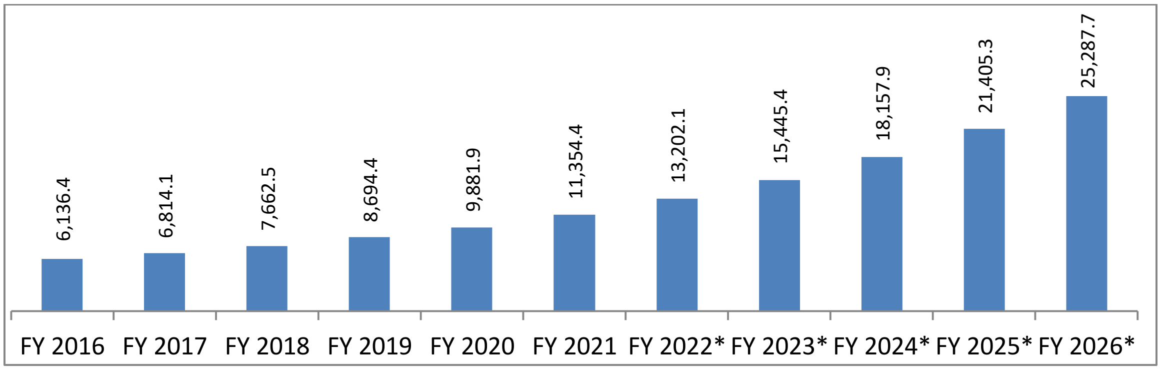
4. Market Size and Forecast for Digital Security and Paperless Transformation

4.1. Global

The global Digital Security and Paperless Transformation market was valued at $11354.4 Mn. by the end of FY 2021 (ending March 2021) and is expected to grow at CAGR 17.4% to value at $25287.7 Mn. by the end of FY 2026. By definition, Digital Security and Paperless Transformation include Digital Trust Services, Digital Security Solutions, and Paperless Transformation Solutions.

- **Digital Trust Services:** Includes 3 components:
  - SSL/TLS Certificates
  - Digital Signature Certificates
  - IoT Certificates
- **Digital Security Solutions:** Includes 2 components
  - Identity and Access Management
  - PKI
- **Paperless Transformation Solutions:**
  - eSignature Workflows

Figure 31: Digital Security and Paperless Transformation Market ($ Mn.), Global, FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
13.1%	**17.4%**

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

The global Digital Security Solutions market is the biggest among the three followed by global Paperless Transformation and global Digital Trust Services market. Identity and Access Management (which includes authentication) is the strongest contributor for the Digital Security Solutions market.

Figure 32: Digital Security and Paperless Transformation Market by Application Type ($ Mn.), Global, FY 2016 – FY 2026

	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022*	FY 2023*	FY 2024*	FY 2025*	FY 2026*
Global Digital Trust Services											
Rev. ($ Mn.)	565.3	664.7	788.1	938.9	1,039.6	1,168.1	1,303.8	1,447.4	1,601.8	1,770.6	1,961.0
YoY (%)		17.6%	18.6%	19.1%	10.7%	12.4%	11.6%	11.0%	10.7%	10.5%	10.8%
Global Digital Security Solutions											
Rev. ($ Mn.)	4,820.9	5,249.5	5,759.2	6,355.4	7,060.7	7,875.8	8,875.6	10,060.6	11,464.7	13,116.2	15,086.6
YoY (%)		8.9%	9.7%	10.4%	11.1%	11.5%	12.7%	13.4%	14.0%	14.4%	15.0%
Global Paperless Transformation Solutions											
Rev. ($ Mn.)	750.2	899.9	1,115.2	1,400.1	1,781.6	2,310.5	3,022.7	3,937.5	5,091.4	6,518.5	8,240.0
YoY (%)		20.0%	23.9%	25.5%	27.2%	29.7%	30.8%	30.3%	29.3%	28.0%	26.4%
Total Digital Security and Paperless Transformation Market											
Rev. ($ Mn.)	6,136.1	6,814.1	7,662.5	8,694.4	9,881.9	11,354.4	13,202.1	15,445.4	18,157.9	21,405.3	25,287.7
YoY (%)		11.0%	12.5%	13.5%	13.7%	14.9%	16.3%	17.0%	17.6%	17.9%	18.1%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

North America remains the largest in the Digital Security and Paperless Transformation market space. Americas (which includes North America and South America) currently contributes to 54.4% of the global market. Strong growth at CAGR 14.9% is expected in the next 5 years. Other regions like APAC and Europe would grow the fastest. India is expected to be one among the fastest growing markets at CAGR 27.5%, ahead of the developed economies. MEA (Middle East and Africa) is likely to grow at CAGR 17.8% till FY 2026 – faster than the growth recorded in the last 5 years. The GCC countries (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates) would be the strongest contributers.

Figure 33: Digital Security and Paperless Transformation Market by Application Type ($ Mn.), Global, FY 2016 – FY 2026

	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022*	FY 2023*	FY 2024*	FY 2025*	FY 2026*
Americas											
Rev. ($ Mn.)	3,262.1	3,628.4	4,092.9	4,666.2	5,338.8	6,180.9	7,055.5	8,046.6	9,247.3	10,710.0	12,388.1
YoY (%)		11.2%	12.8%	14.0%	14.4%	15.8%	14.1%	14.0%	14.9%	15.8%	15.7%
Europe											
Rev. ($ Mn.)	1,311.7	1,457.6	1,642.3	1,869.9	2,129.5	2441.7	2,874.3	3,439.6	4,133.9	4,941.7	5,915.1
YoY (%)		11.1%	12.7%	13.9%	13.9%	14.7%	17.7%	19.7%	20.2%	19.5%	19.7%
APAC											
Rev. ($ Mn.)	1,108.7	1,243.5	1,392.5	1,569.8	1,771.0	2,000.7	2,422.6	2,964.1	3,588.9	4,359.7	5,324.6
YoY (%)		12.2%	12.0%	12.7%	12.8%	13.0%	21.1%	22.4%	21.1%	21.5%	22.1%
MEA											
Rev. ($ Mn.)	453.8	484.6	534.8	588.5	642.5	731.1	849.7	995.1	1,187.8	1,393.9	1,659.8
YoY (%)		6.8%	10.3%	10.0%	9.2%	13.8%	16.2%	17.1%	19.4%	17.3%	19.1%
Total Digital Security and Paperless Transformation Market											
Rev. ($ Mn.)	6136.4	6814.1	7662.5	8694.4	9,881.9	11,354.4	13,202.1	15,445.4	18,157.9	21,405.3	25,287.7
YoY (%)		11.0%	12.5%	13.5%	13.7%	14.9%	16.3%	17.0%	17.6%	17.9%	18.1%

*Projected, Base Year is FY 2021, Americas = includes North America and South America; Europe = includes Western Europe, Eastern Europe and UK; APAC = includes South Asia, ANZ, China/GCR and other east Asian coutries; MEA = includes Middle East and African countries

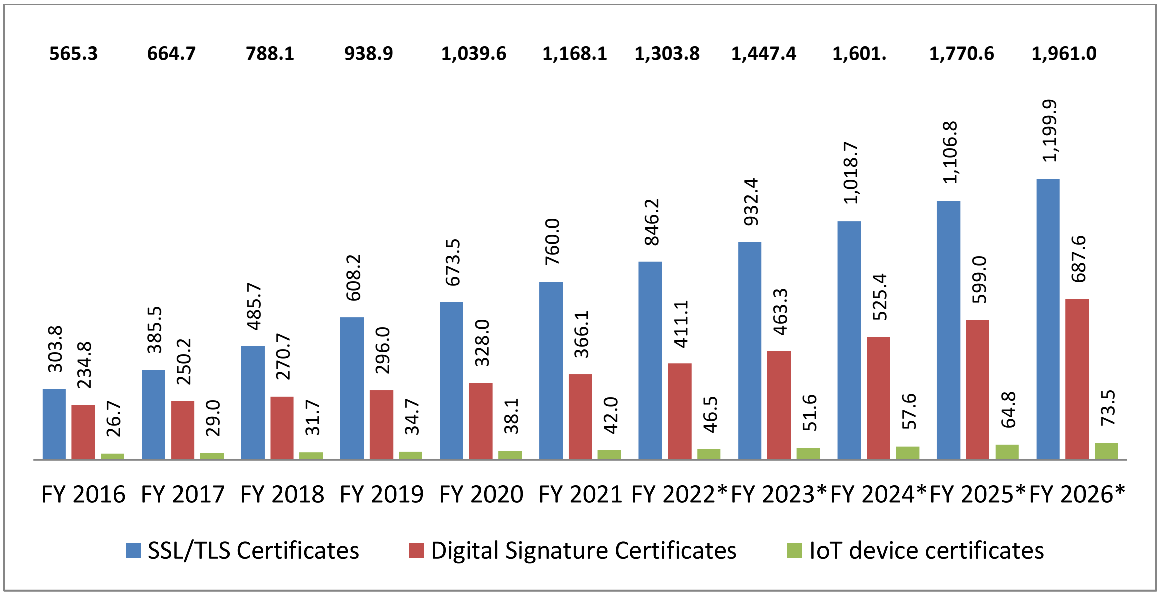
Source : Frost & Sullivan

Digital Trust Services Market

Market Size and Forecast

The Digital Trust Services market which includes SSL/TLS certificates, Digital Signature Certificates and IoT device certificates has strong growth potential. SSL/TLS certificates contribute to 65.1% of the market and valued at $760.0 Mn. by the end of FY 2021. Historically the market has grown at a CAGR of 20.1% from FY 2016 to FY 2021. Digital Signature Certificates market has grown at 9.3% in the last 5 years. However, growth projections look strong till FY 2026 and expected to grow at a CAGR of 13.4%. IoT is fast growing market and would push the need for device certificates. The IoT device certificates market is expected to grow in double digits in the next 5 years.

Figure 34: Global Digital Trust Services Market ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Global Digital Trust Services	15.6%	10.9%
SSL/TLS Certificates	20.1%	9.6%
Digital Signature Certificates	9.3%	13.4%
IoT Device Certificates	9.5%	11.8%

*Projected, Base Year is FY 2021

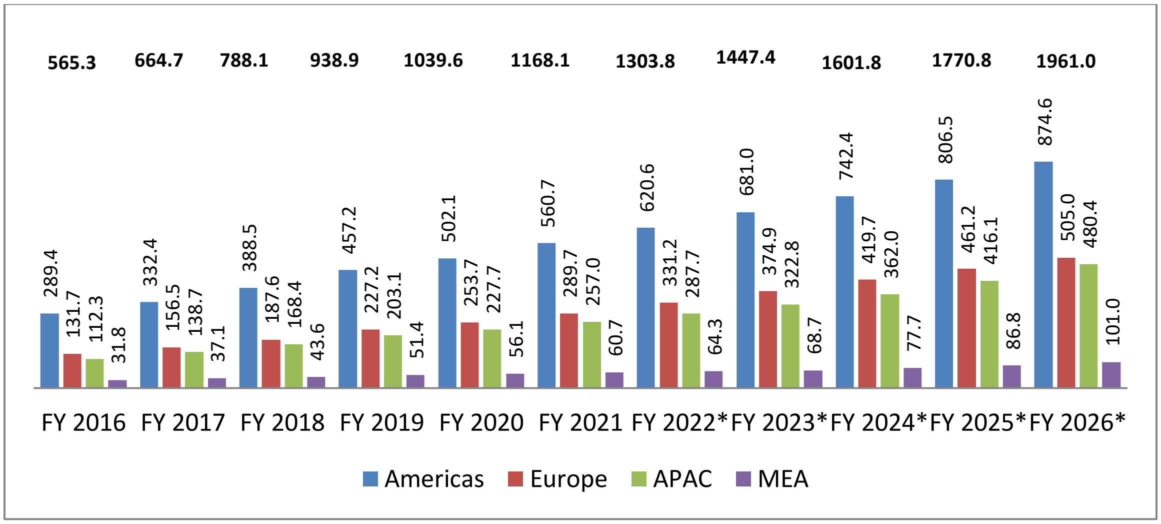
The revenue of players who bundle Digital Signature offering with paperless transformation/workflow (like DocuSign) have been segmented under Paperless Transformation Solutions market

Source : Frost & Sullivan

Geographical Analysis

As on FY 2021, Americas remains the biggest market contributing to 48.0% of the Global Digital Trust Services market to value $560.7 Mn. Growth is expected to be in the lines of CAGR 9.3% till FY 2026 making it still the largest market. The existing revenue base for the region remains strong and near double digit revenue growth is considered healthy. USA is the biggest market contributor in the region as enterprises remain conscious over cybersecurity and digital identity. Europe remains the second biggest market with close competition from APAC. China, South Korea, Japan, Singapore and Australia are the biggest markets; India remains one among the fastest growing in the region. Africa (except for South Africa) remains behind in terms of adoption thereby contributing less to the MEA market share.

Figure 35: Global Digital Trust Services Market by Key Geographies ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Americas	14.1%	9.3%
Europe	17.1%	11.8%
APAC	18.0%	13.3%
MEA	13.8%	10.7%

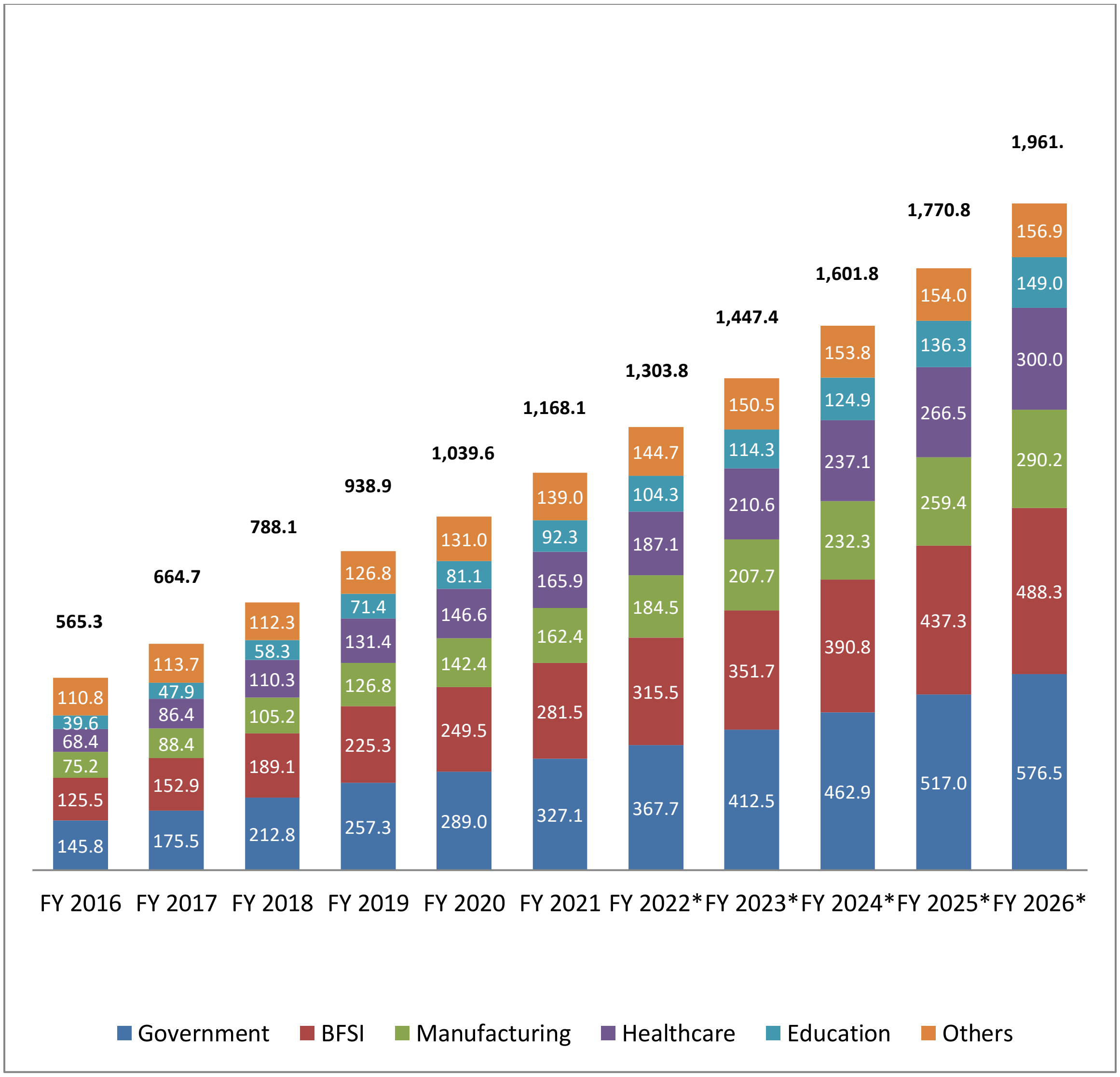
*Projected, Base Year is FY 2021

Source : Frost & Sullivan

Industry Vertical Analysis

The Government vertical is the biggest contributor for the Digital Trust market. The demand is mostly driven by the use of Digital Signature Certificates. Citizens can access government schemes by proving their identity and using digital signatures. People can file income tax returns, file patents and take part in e-auctions using digital signatures. Likewise in BFSI, banks and customers can sign e-policies, by digitally signing documents which is considered as legal bindings.

Figure 36: Global Digital Trust Services Market by Industry Verticals ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	17.5%	12.0%
BFSI	17.5%	11.6%
Manufacturing	16.6%	12.3%
Healthcare	19.4%	12.6%
Education	18.5%	10.1%
Others	4.6%	2.4%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

Players having presence in the Global Market

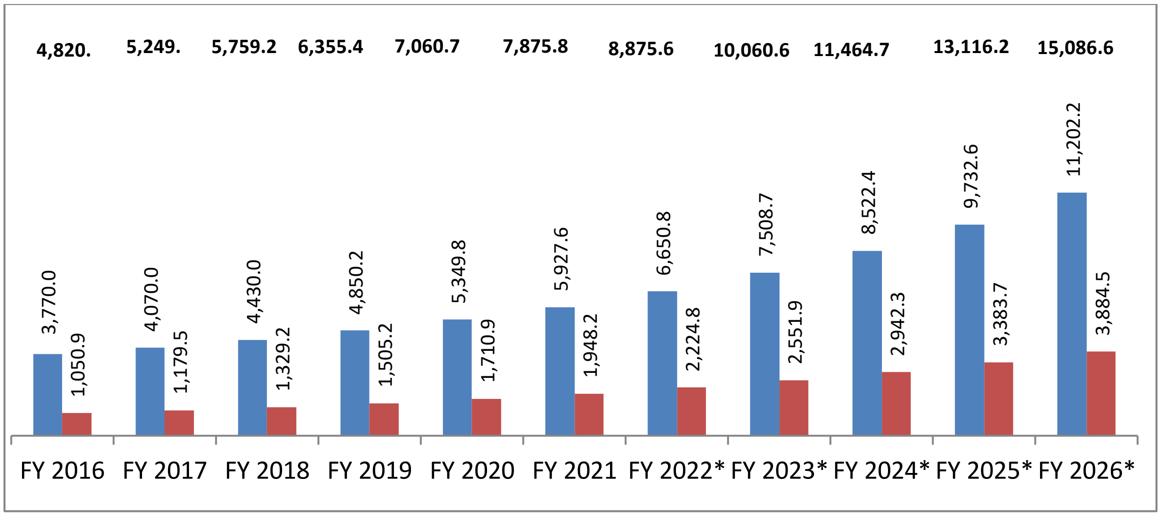
- **SSL/TLS Certificate Market :** DigiCert (USA), Sectigo (USA), Entrust (USA), GlobalSign (Belgium), GoDaddy (USA), Network Solutions (USA), Trustwave (USA), SwissSign (Switzerland), RapidSSL (USA), eMudhra (India), etc.
- **Digital Signature Certificates Market :** IdenTrust (USA), Comodo (USA), DigiCert (USA), GoDaddy (USA), GlobalSign (Belgium), ACTALIS (Italy), Entrust (USA), Trustwave (USA), SwissSign (Switzerland), WISeKey (Switzerland), eMudhra (India), etc.
- **IoT Device Certificates Market :** GlobalSign (Belgium), Comodo (USA), DigiCert (USA), Sectigo (USA), Entrust (USA), eMudhra (India), etc.

Digital Security Solutions Market

Market Size and Forecast

The Digital Security Solutions market comprises of Identity and Access Management and PKI. With digital transformation holding center stage, the relevance and importance of IAM and authentication services have increased multi-fold. Frauds around digital identity have increased and concepts like zero trust security architectures have emerged. The acceptance of cloud technologies has even pushed forward the need for IAM and authentication. It is estimated that the global digital security solutions market is valued at $7875.8 Mn. by the end of FY 2021. IAM contributes to 75.3% of the market followed by 24.7% by PKI.

Figure 37: Global Digital Security Solutions Market ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Global Digital Security Solutions	10.3%	13.9%
Identity and Access Manegement (IAM)	9.5%	13.6%
Public Key Infrastructure (PKI)	13.1%	14.8%

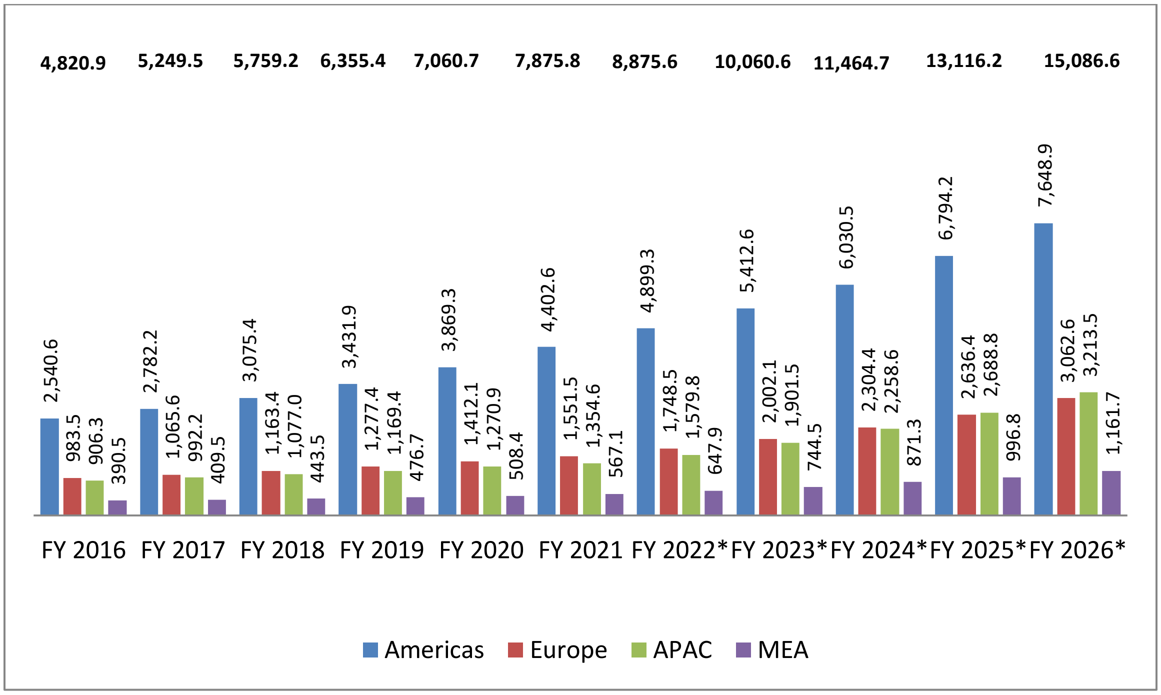
*Projected, Base Year is FY 2021

Source : Frost & Sullivan

Geographical Analysis

Americas currently contributes to 55.9% of the overall Digital Security Solutions market and is valued at $4402.6 Mn. Double digit growth (CAGR 11.7%) is expected to continue till the end of FY 2026. The higher level of maturity of companies in USA has pushed foward the demand for authentication and IAM solutions. As other regions have started to focus strongly on digital initiatives, the need for IAM solutions will increase globally. APAC is likely to be the fastest growing region with a CAGR of 18.9%. Driven by strong growth in Western Europe, the region (Europe) will see strong adoption and likely to hold on to its market share at 20.3% by the end of next 5 years. The Smart Cities initiatives in Middle East would push forward the demand for IAM and PKI solutions.

Figure 38: Global Digital Security Solutions Market by Key Geographies ($ Mn.),
FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Americas	11.6%	11.7%
Europe	7.7%	15.4%
APAC	9.5%	14.6%
MEA	8.4%	18.9%

*Projected, Base Year is FY 2021

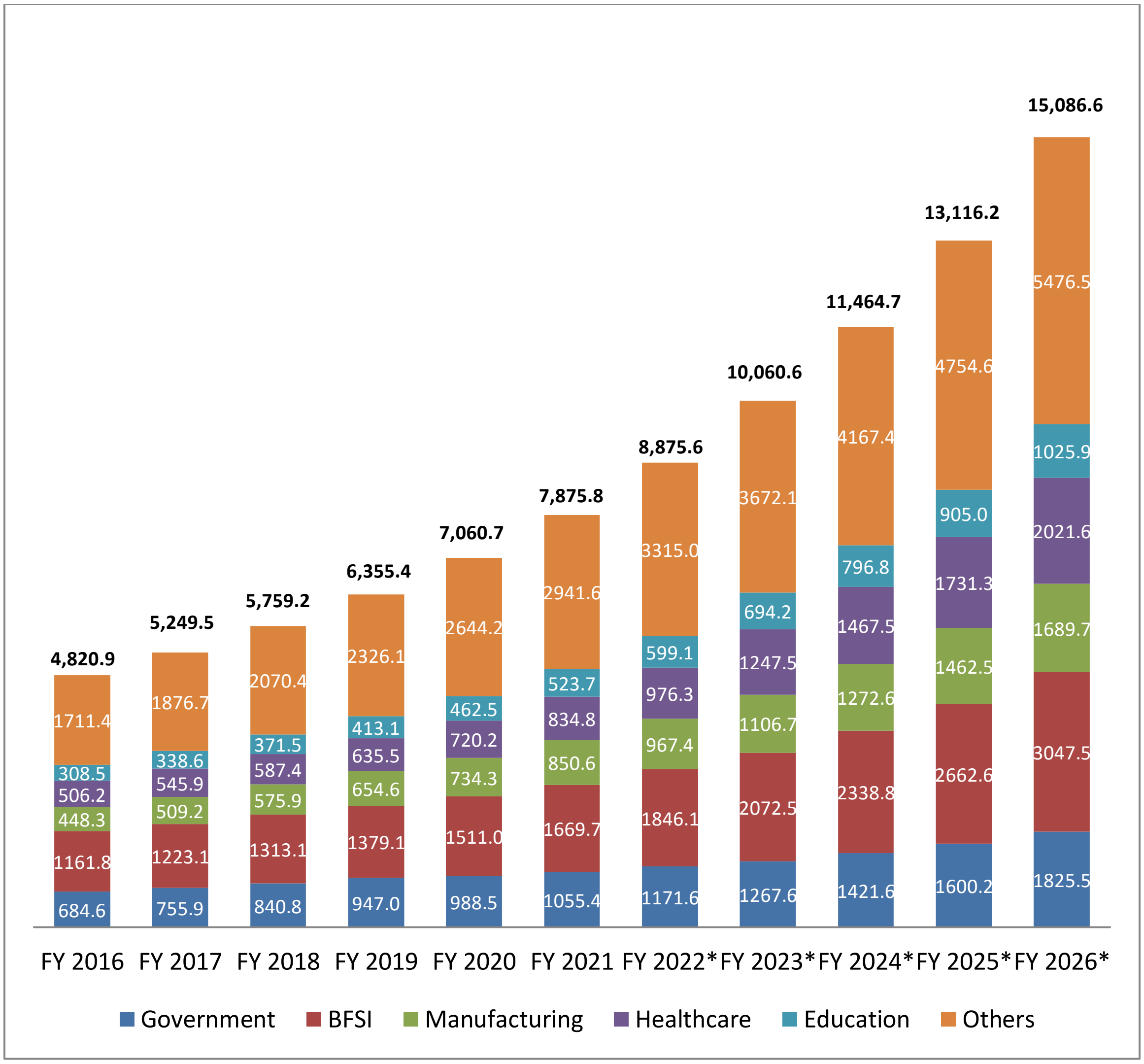
Source : Frost & Sullivan

Industry Vertical Analysis

BFSI is the biggest user of Digital Security Solutions. The high level of sensitive financial data calls for the strongest authentication and IAM techniques. Bank frauds have increased and hence banks have resorted to advanced authentication techniques like SSO, MFA, OTP, digital signature, knowledge based authentication, etc.

Demand for authentication has also increased in government as citizen welfare schemes have been launched. To avail the public welfare schemes and to avoid fraud, users are required to prove their identity using authentication techniques.

Figure 39: Global Digital Security Solutions Market by Industry Verticals ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	9.0%	11.6%
BFSI	7.5%	12.8%
Manufacturing	13.7%	14.7%
Healthcare	10.5%	19.3%
Education	11.2%	14.4%
Others	11.4%	13.2%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

Players having presence in the Global Market

- **IAM Market :** Microsoft (USA), IBM (USA), Ping Identity (USA), Okta (USA), Sailpoint (USA), Ilantus technologies (USA), Saviynt (USA), Thales (France), Broadcom (USA), eMudhra (India), etc.
- **PKI Market :**
  - **Hardware:** Thales (France), HID Global (USA), Keyfactor (USA), etc.
  - **Software:** Entrust (USA), Nexus Group (Sweden), eMudhra (India), etc.
  - **Certificate Discovery :** DigiCert (USA), Sectigo (USA), AppViewX (USA), Venafi (USA), eMudhra (India), etc.
  - **Cloud Infrastructure :** Google (USA), AWS (USA), etc.

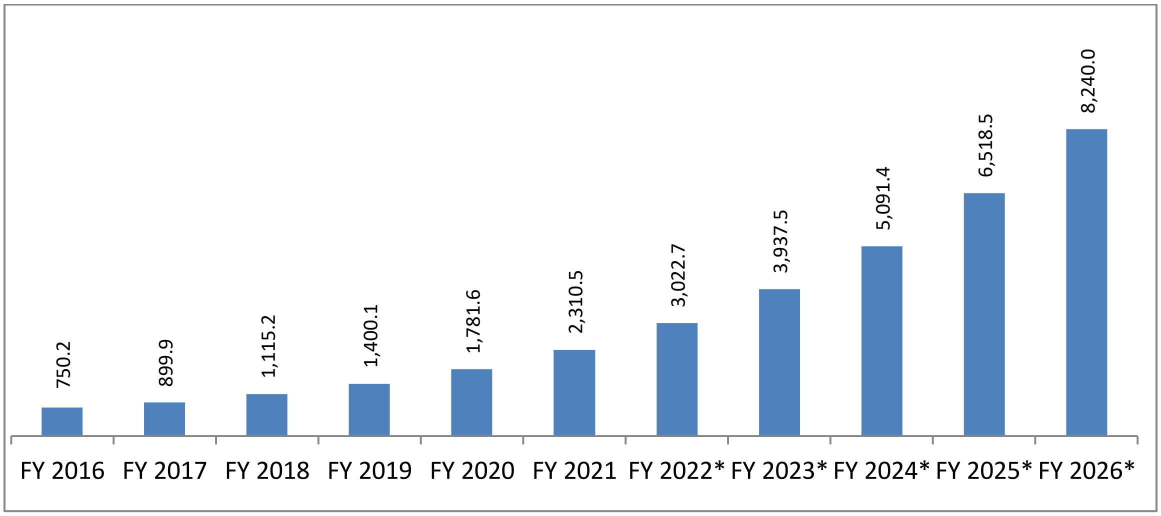
Paperless Transformation Solutions Market

Market Size and Forecast

Paperless office and work-process is expected to be future of global enterprises. Companies aim to reduce manual interventions and automate customer and internal processes. This requires serious focus around digitization and workflow solutions that improve efficiency and cut down physical paper needs.

Frost & Sullivan estimates the current paperless transformation solutions market (which includes workflows) to be valued at $2310.5 Mn. Growth is expected to be exponential in the next 5 years touching a CAGR of 29.0%. By FY 2026, the global paperless transformation market is expected to grow over 3x to reach $8240.0 Mn.

Figure 40: Global Paperless Transformation Solutions Market ($ Mn.), FY 2016 – FY 2026



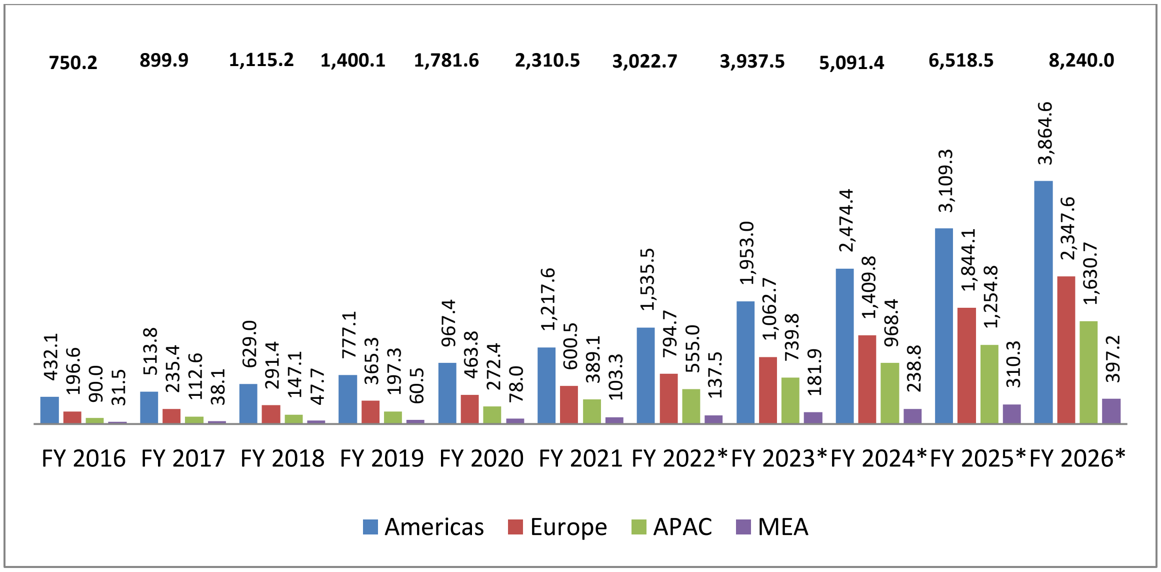
CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
25.2%	29.0%

*Projected, Base Year is FY 2021
Source : Frost & Sullivan

Geographical Analysis

Americas currently has a market share of 52.7% and is valued at $1217.6 Mn. In the last year, the market has grown at 25.9%. US based enterprises have been strongly focusing on automation and finding ways to introduce paperless workflows within their customer onboarding and internal processes. Paperless workflows eleminate the need for physical presence of customers and improve turnarounds. Europe currently has a revenue share of 26.0% which is expected to grow even further to 28.5% in the next 5 years. APAC currently has a market contribution of $389.1 Mn. and expected to be the fastest growing (CAGR 33.2%) geography during the forecast period.

Figure 41: Global Paperless Transformation Solutions Market by Key Geographies ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Americas	23.0%	26.0%
Europe	25.0%	31.3%
APAC	34.0%	33.2%
MEA	26.8%	30.9%

*Projected, Base Year is FY 2021

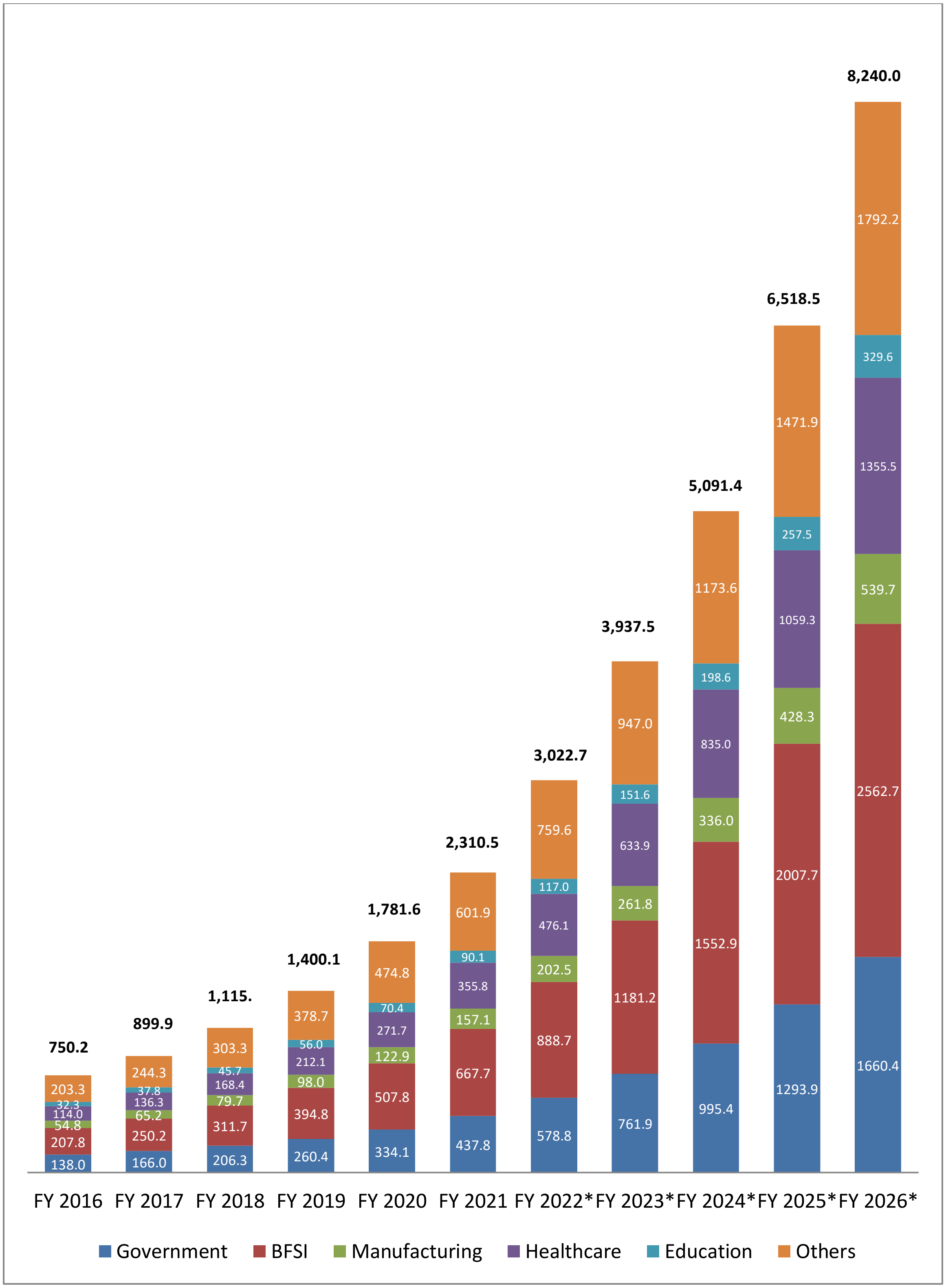
Source : Frost & Sullivan

Industry Vertical Analysis

BFSI companies are the largest users of paperless transformation solutions. The industry vertical is highly regulated with strict procedures and guidelines. Manual processes make things complicated and time taking and hence it is required for self service modes in the BFSI industry. Customers should be able to fill up and sign forms online instead of visiting banks and submitting them physically. The progress over paperless transformation has been steady and likely to increase even further in the next 5 years. BFSI is estimated to grow at CAGR 30.9% till FY 2026 to value $2562.7 Mn. due to growing online frauds, and rising security concerns.

Apart from the BFSI industry, government is another sector that is likely to strong impact of paperless transformation solutions. Governments across the world are working towards leveraging technologies to improve citizen services. Various digital initiatives have been launched spending huge amount of money, which requires designing processes well without compromising on security. The high risk of fraud amidst increasing digitalization of banking transactions aids demand for digital signatures By FY 2026, the government vertical is likely to grow at a CAGR of 30.6% to become a market of $1660.4 Mn.

Figure 42: Global Paperless Transformation Solutions Market by Industry Verticals ($ Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	26.0%	30.6%
BFSI	26.3%	30.9%
Manufacturing	23.5%	28.0%
Healthcare	25.6%	30.7%
Education	22.8%	29.6%
Others	24.2%	24.4%

*Projected, Base Year is FY 2021
Source : Frost & Sullivan

Players having presence in the Global Market

- **Paperless Transformation/Workflow Solutions Market :** Adobe (USA), OneSpan (USA), DocuSign (USA), Alpha Trust (USA), WISeKey (Switerland), eMudhra (India), etc.

4.2. India

India remains one of the fastest growing Digital Security and Paperless Transformation markets in the world. The Government of India has been agressive in terms of leveraging digital transformation in its various initiatives. The aim is to bring down corruption, red tapism, improve process efficiency and quicker turn arounds on service delivery without compromising on security. The Digital India (DI) program is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy. The DI schemes make use of advanced technologies like automation, artificial intelligence, paperless workflows, and digital signatures to streamline processes and improve error-free outcomes. Paperless workflows are designed to improve the overall user experience while creating a single source of truth for compliance. Through the concept of paperless workplace, convenience, compliance and cost can be taken into account. In the entire chain of processes, authentication remains the most important critical factor. Aadhaar linked accounts make sure identity fraud is avoided. From filing GST, income tax returns to passport renewal and ration cards; digital identity is a pivotal instrument.

BFSI is another industry segment that has seen early success/usage of digital security and paperless transformation. Both public and private sector banks in India have started to eliminate traditional processes of paper based applications and trasactions to digital processes. Digitization in banks enables better customer experience, improve digital presence, and refine internal process alignment with minimal manual intervention. eKYC and Aadhaar Enabled Payment Systems are two of the important applications of authentication in the Indian banking system.

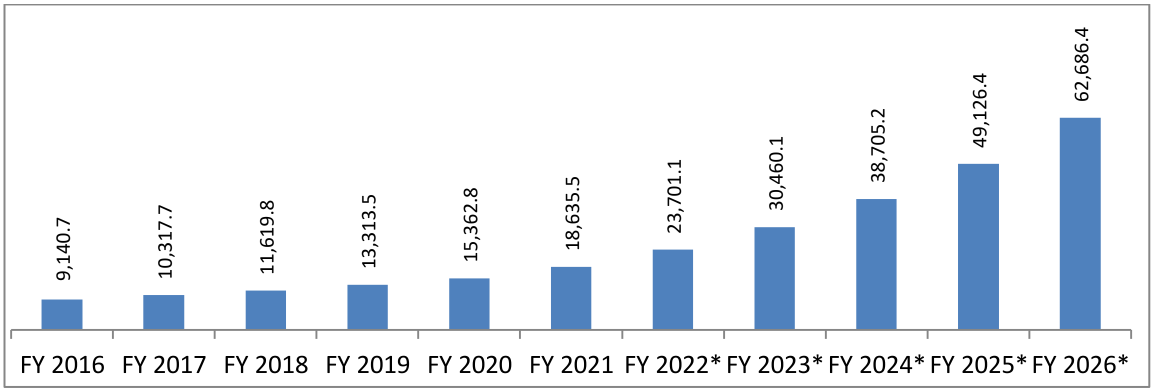
The Digital Security and Paperless Transformation market can be tracked at 2 levels:

(1) at the OEM level (the revenue that the OEM/solution providers generate) : This is revenue registered at the solution provider's India book of accounts

(2) at the end-user level (the revenue that the channel partners clock in by re-selling the solution to the end users) : Most of the Digital Security and Paperless Transformation market solution providers take a channel driven approach to sell products to end users in India. The additional mark up cost that channel partners add to the original cost of the product includes applicable taxes. In few cases (like digital signature certificates), the channel partners buy the solution in bulk at a much lower price and sell it off to the end-users/in the retail market at much higher rates.

The Indian Digital Security and Paperless Transformation market at the OEM level stands at INR. 18635.5 Mn. by the end of FY 2021. Historically the market has grown at CAGR 15.3% since FY 2016 and likely to grow at CAGR 27.5% in the next 5 years.

Figure 43: Digital Security and Paperless Transformation Market – At OEM Level (INR. Mn.), India, FY 2016 – FY 2026



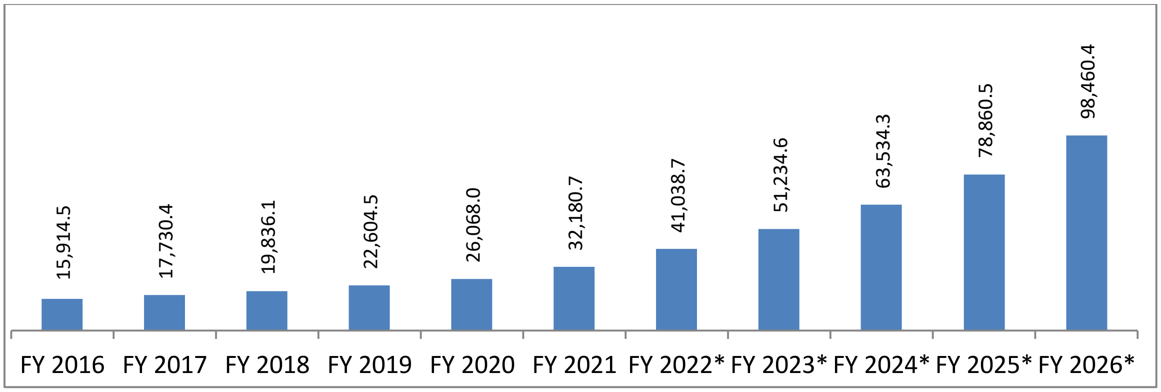
CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
15.3%	27.5%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

At the end-user level, the market is currently valued at INR. 32180.7 Mn. in FY 2021, a value much higher than the actual OEM level market. The huge difference is due to the high cost difference at which digital signature certificates are sold to the end-users by the channel partners. Till FY 2026, the market at the end-user level is likely to grow at CAGR 25.1%.

Figure 44: Digital Security and Paperless Transformation Market – At End-user Level (INR. Mn.), India, FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
15.1%	**25.1%**

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure

Source : Frost & Sullivan

The Indian Digital Security Solutions market (which includes IAM and PKI) is the biggest contributor of the Digital Security and Paperless Transformation market. IAM is the single largest revenue pocket within all sub-segments of the market. Digital Trust and Paperless Transformation contribute to 20.3% and 15.1% of the overall market respectively. Growth of Digital Trust Services is expected to be 17.1% in the next 5 years as against 15.9% in the last 5. This high growth will primarily be driven by strong use of digital signature certificates across industries like Govt. and BFSI in India. Also, as the number of IoT devices increase, enterprises would be bothered about their security and hence look towards IoT device certificates. The growing number of cyber-attacks would be a strong growth driver for the Indian SSL/TLS market in the years to come.

Figure 45: Digital Security and Paperless Transformation Market by Application Type (INR. Mn.) – At OEM Level, India, FY 2016 – FY 2026

	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022*	FY 2023*	FY 2024*	FY 2025*	FY 2026*
India Digital Trust Services											
Rev. (INR Mn.)	1802.9	2091.8	2423.1	2815.8	3264.1	3777.3	4369.8	5071.2	5922.2	6973.5	8326.2
YoY (%)		16.0%	15.8%	16.2%	15.9%	15.7%	15.7%	16.1%	16.8%	17.8%	19.4%
India Digital Security Solutions											
Rev. (INR Mn.)	6111.5	6837.2	7581.3	8578.6	9794.2	12045.4	15804.1	20852.9	26777.4	33871.2	42384.8
YoY (%)		11.9%	10.9%	13.2%	14.2%	23.0%	31.2%	31.9%	28.4%	26.5%	25.1%
India Paperless Transformation Solutions											
Rev. (INR Mn.)	1226.4	1388.6	1615.4	1919.2	2304.5	2812.7	3527.2	4536.0	6005.6	8281.7	11975.4
YoY (%)		13.2%	16.3%	18.8%	20.1%	22.1%	25.4%	28.6%	32.4%	37.9%	44.6%
Total Digital Security and Paperless Transformation Market											
Rev. (INR Mn.)	9140.7	10317.7	11619.8	13313.5	15362.8	18635.5	23701.1	30460.1	38705.2	49126.4	62686.4
YoY (%)		12.9%	12.6%	14.6%	15.4%	21.3%	27.2%	28.5%	27.1%	26.9%	27.6%

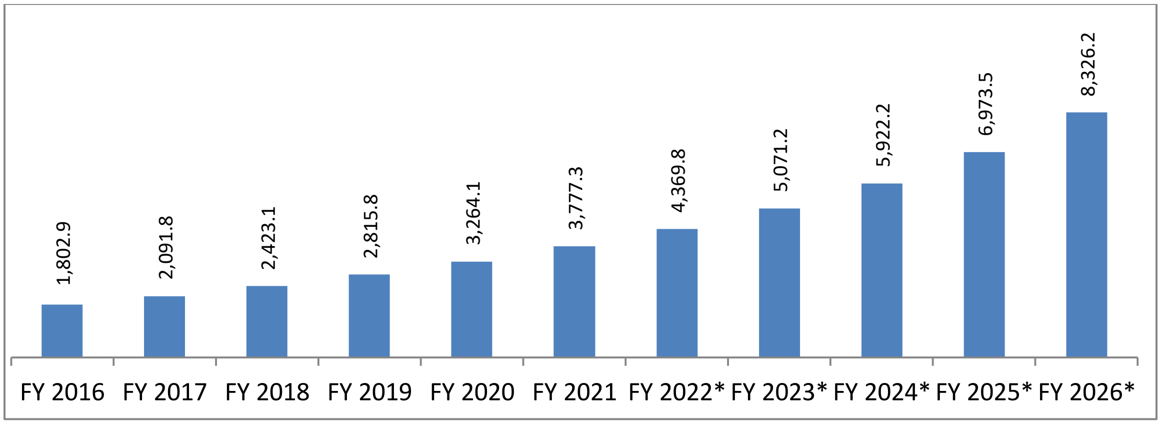
*Projected, Base Year is FY 2021
Source : Frost & Sullivan

Digital Trust Services Market

Market Size and Forecast

The Indian Digital Trust Services market is currently valued at INR. 3777.3 Mn. in FY 2021 at the OEM level. Since FY 2016 till FY 2021, the market has grown at a CAGR of 15.9%. Growth till FY 2026 is expected to be even faster than the last 5 years (likely to be CAGR 17.1%) due to stronger adoption of digital technologies in enterprise processes and government initiatives.

Figure 46: India Digital Trust Services Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
15.9%	**17.1%**

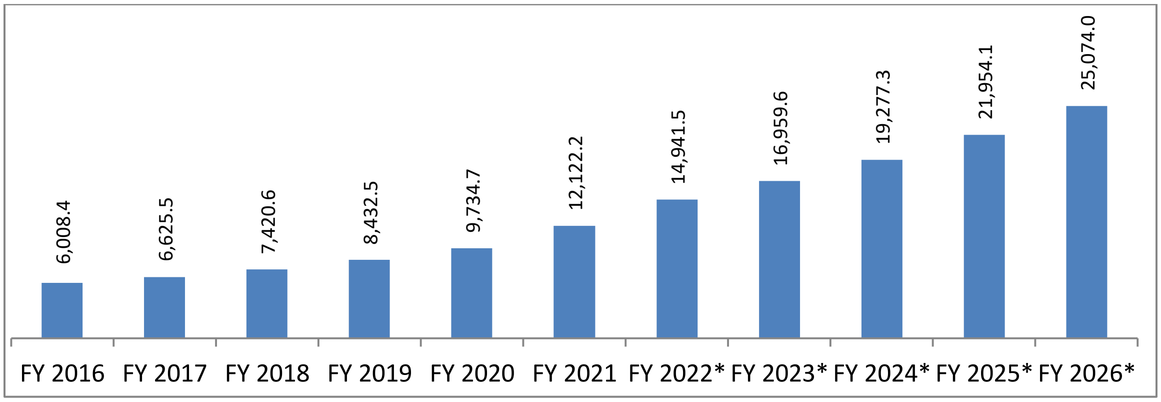
*Projected, Base Year is FY 2021

Source : Frost & Sullivan

The high growth potential of the market, lure Digital Trust vendors to explore opportunities. Companies/vendors who have a wide portfolio of offerings are likely to excel and mine the existing opportunities. The stakeholders in the market currently include local licensed CAs (certifying authorities) and few global players/CAs. Just a few stakeholders in the market have a larger focus on all the segments of Digital Trust Services, while others play in specific areas – eMudhra happens to be a vendor with a broad portfolio of offerings.

The Indian Digital Trust Services market at the end-user level is currently valued at INR. 12122.2 Mn. and expected to grow at CAGR 15.6% in the next 5 years. From FY 2016 till FY 2021, the market is recorded to have grown by 15.1%.

Figure 47: India Digital Trust Services Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
15.1%	**15.6%**

* Projected, Base Year is FY 2021, end-user revenue estimated at constant tax structure
Source : Frost & Sullivan

eMudhra is one of the strongest players in the Indian Digital Trust Services market with a market share of 17.8% in FY 2021. The company is estimated to have grown at 19.6% from FY 2020 (based on eMudhra's financial report), much higher than the market average growth of 15.7% for the segment at the OEM level. Being the largest Certifying Authority (CA) in India, the company's growth comes from its dominance in the Digital Signature Certificates market with a market share of 37.9% which clearly proves eMudhra's supremacy in the market.

With several milllions DSCs issued, eMudhra caters to all kind of subscribers who use digital certificates for income tax return filing, MCA (RoC), tenders, foreign trade, banking, railways and many other needs. The company works closely with large government and banking customers like the Reserve Bank of India, Defence Forces, 20+ public and private sector banks and state governments.

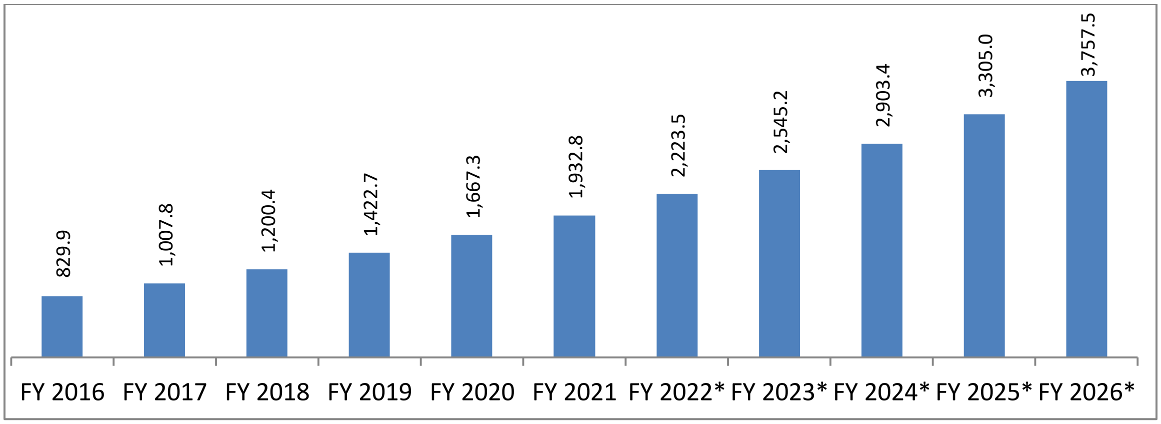
The strong relationship that eMudhra has crafted with 80,000+ channel partners and leading system integrators in India has been instrumental in penetrating into several of the large enterprise accounts and reaching out to end users. Headquartered in the Silicon Valley of India, Bengaluru, and having local presence in 7 of India's cities make eMudhra work very closely with customers by understanding their needs and delivering as per their expectations. The company understands the strong global market opportunity that Digital Trust Services offer and hence have started to make inroads in other geographies with presence in Middle East (Dubai), APAC (Malaysia, Indonesia, North America (New Jersey, Florida), Latin America (Bogota), and Europe (Amsterdam).

Market Size and Forecast by Digital Trust Service Applications

- **SSL/TLS Certificates Market in India**

The Indian SSL/TLS Certificates market is valued at INR. 1932.8 Mn. in FY 2021. As enterprises increase their online presence and create a digital footprint, it becomes obvious to make sure that websites are secured. Volumes of data reside on these websites and users rely on them to transact. Without a website, companies often lose to have a mind share among customers. eCommerce and digital banking are significant digital trends that India has seen in the recent past. SSL/TLS help encrypt information sent over the internet and they provide identity assurance, both of which help online consumers to positively identify and trust websites that are safe to transact with. Today, most of the secured websites of the world have's' included after using 'HTTP' to convey that the site is secured and digitally trusted. Browsers now issue strong warnings to visitors who try to enter websites that are not secured by HTTPS. SSL/TLS certificates also help websites achieve better SEO ranking which is critical in the competitive world.

Figure 48: India SSL/TLS Certificates Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026

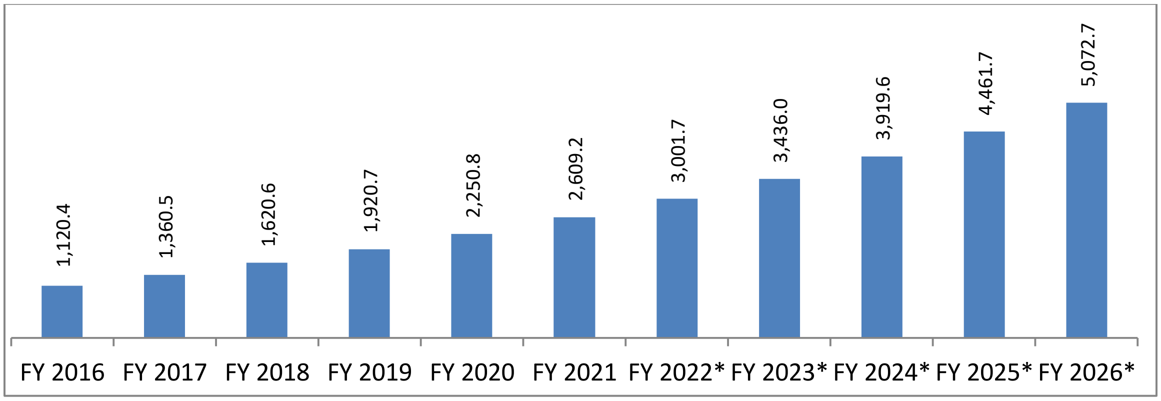


CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.4%	14.2%

*Projected, Base Year is FY 2021
Source : Frost & Sullivan

Channel partners have an average of 35% markup when they sell SSL/TLS certificates to customers in India.

Figure 49: India SSL/TLS Certificates Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.4%	14.2%

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure
Source : Frost & Sullivan

eMudhra has been quick to identify the huge market opportunity that lies in the Indian SSL/TLS certificates market. It has recently started selling SSL certificates to all type of customers. The Secure DV (domain validation) certificates are aimed at websites, blogs, personal sites and non-business websites. It comes with HTTPS and secure padlock. The Secure OV (organization validation) certificates are meant for small business and organizations and come with HTTPS, secure padlock and business information authentication services. The last variant, Secure EV (extended validation) is meant for e-commerce websites or websites holding sensitive information and comes with HTTPS, secure padlock and organization details in the address bar. Most of these certificates come with 1 year validity and at the price point that makes it affordable for most.

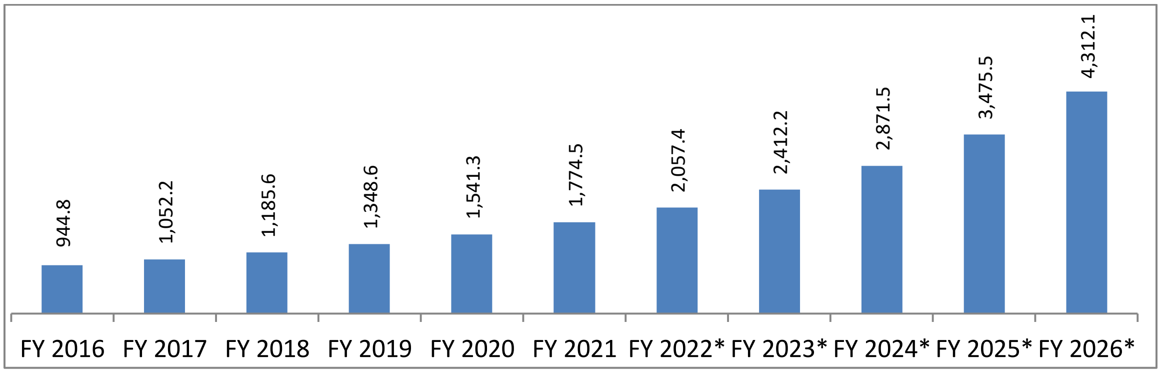
The biggest advantage that eMudhra has over its competitors is the fact that it is the largest licensed CA in India with strong DSC expertise which would make eMudhra penetrate into the market much easily than it competitors. eMudhra is the only Indian company to be directly recognized by renowned browsers and document processing software companies such as like Microsoft, Mozilla, Apple and Adobe allowing eMudhra to sell digital identities to individual/organization and issue SSL/TLS certificates for website authentication, globally. Also, eMudhra is accredited to WebTrust (again the only Indian company) that make its digital signature certificates directly recognized by browsers across the world allowing eMudhra to issue digital signature certificates in many countries (the aim of WebTrust is to promote confidence and trust between consumers and businesses on the Internet.)

- **Digital Signature Certificates Market in India**

The Certifying Authorities (CAs) issue Digital Signature Certificates to enterprises and users. As per the Information Technology Act 2000, documents submitted in electronic form need to have Digital Signatures to ensure security and authenticity of the documents filled electronically. DSCs are mandatory while filing income tax returns, GST, e-tendering, patent and trademark filing, MCA e-filing, LLP registration, customs e-filing, e-procurement, e-bidding, and e-auction. It is allowed to use Digital Signatures issued to a particular individual and is illegal to use Digital Signatures of some other person. DSCs are typically issued with one year and two years validity. These certificates can be renewed on expiry of the period of initial issue. DSC applicants can directly approach CAs with original supporting documents and self-attested copies or by using Aadhaar eKYC based authentication.

Frost & Sullivan estimates the Digital Signature Certificates market in India to be valued at INR. 1774.5 Mn. by the end of FY 2021 at the OEM level. The market is estimated to have grown by 13.4% in the last 5 years and expected to growth at CAGR 19.4% till FY 2026. Currently there are 15 licensed CAs in India as per the cca.gov.in website. While the global CAs has a strong market share worldwide, they do not have the license to operate in India.

Figure 50: India Digital Signature Certificates Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
13.4%	19.4%

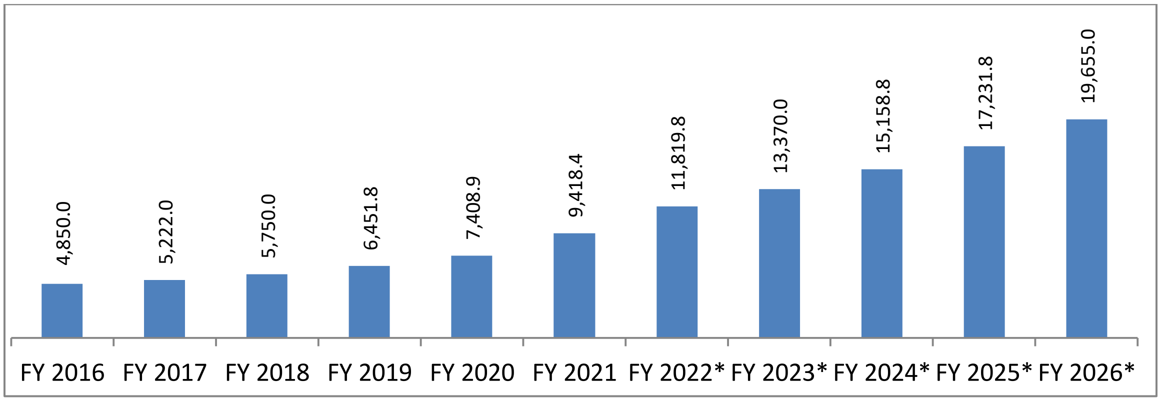
*Projected, Base Year is FY 2021

The revenue of players who bundle Digital Signature offering with paperless transformation/workflow (like DocuSign) have been segmented under Paperless Transformation Solutions market

Source : Frost & Sullivan

DSC is one of the very few markets where resellers/channel partners buy DSCs from licensed CAs in bulk at low price points and sell them to end customers at high values making big profits. The margins could be as big as 5x the original price at which they buy DSCs from the CAs. The retail model works as CAs sell DSCs directly to the end customer through their websites.

Figure 51: India Digital Signature Certificates Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
14.2%	15.9%

*Projected, Base Year is FY 2021, end-user revenue estimated at constant tax structure

The revenue of players who bundle Digital Signature offering with paperless transformation/workflow (like DocuSign) have been segmented under Paperless Transformation Solutions market

Source : Frost & Sullivan

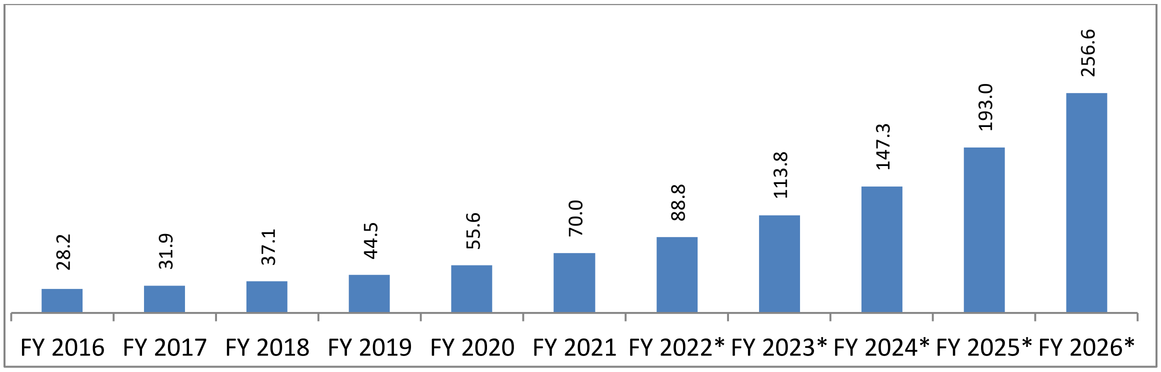
eMudhra remains the largest CA in India with 37.9% market share in the Digital Signature Certificates market space in FY 2021. It is estimated, that the company has grown at 19.6% in FY 2021 (based on eMudhra's financial reporting) as against a market average of 15.1% at the OEM level. The high growth has enabled eMudhra improve on its earlier market share of 36.5% in FY 2020. eMudhra is the only Indian company to be admitted as a member of the European Cloud Signature Consortium as well as Certifying Authority / Browser Forum, a global forum that governs the use of SSL/TLS certificates. Being a member of the aforementioned global forums is a matter of pride for any vendor thereby making eMudhra unique and different from others in the segment.

- **IoT Device Certificates Market in India**

IoT is believed to be one of the strongest pillars of digital transformation. The number of IoT connected devices is estimated to be around 10.07 Bn. in 2021 and 25.44 Bn. by 2030. IoT would find use cases into all major industries starting from commercial to industrial, smart cities and consumer. Opportunities remain huge in IoTas cyber threats remain the biggest concern for these IoT devices. Cyber criminals are likely to target unsecured IoT devices that are placed in remote locations. Miscreants could also plant unauthorized IoT devices into networks to steal data. IoT device certificates help to verify and grant device access to the network. No device could be synced in with the enterprise network without the right authorization. While the market for IoT device certificate is currently small, potential remains high and the opportunity is likely to increase with higher customer awareness over the period of time.

The Indian IoT device certificates market is estimated to be around INR. 70.0 Mn. by the end of FY 2021 and expected to grow at CAGR 29.7% in the next 5 years.

Figure 52: India IoT Device Certificates Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026



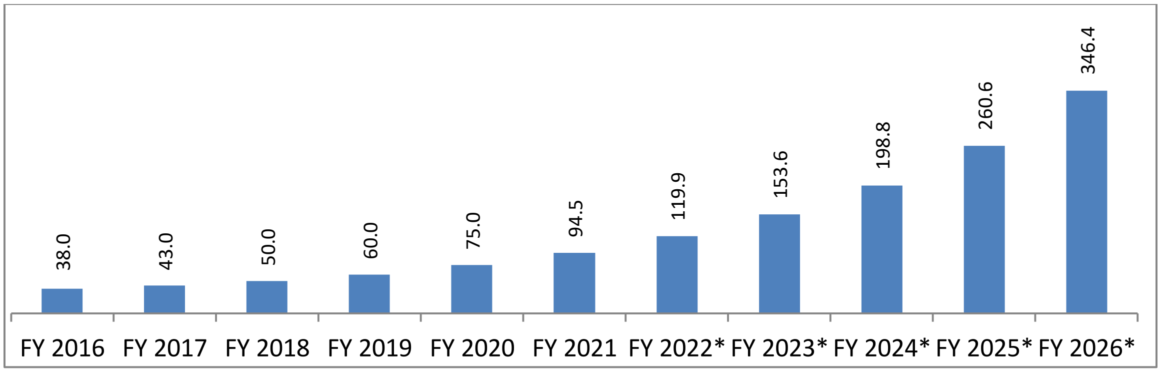
CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
20.0%	**29.7%**

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

IoT Device Certificate solution providers in India take a channel driven strategy to reach out to end customers. Enterprises are the major users of IoT device certificates, not consumers. IoT Device Certificates are often sold to enterprises as part of larger transformation deals where Systems Integrators participate.

Figure 53: India IoT Device Certificates Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
20.0%	**29.7%**

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure

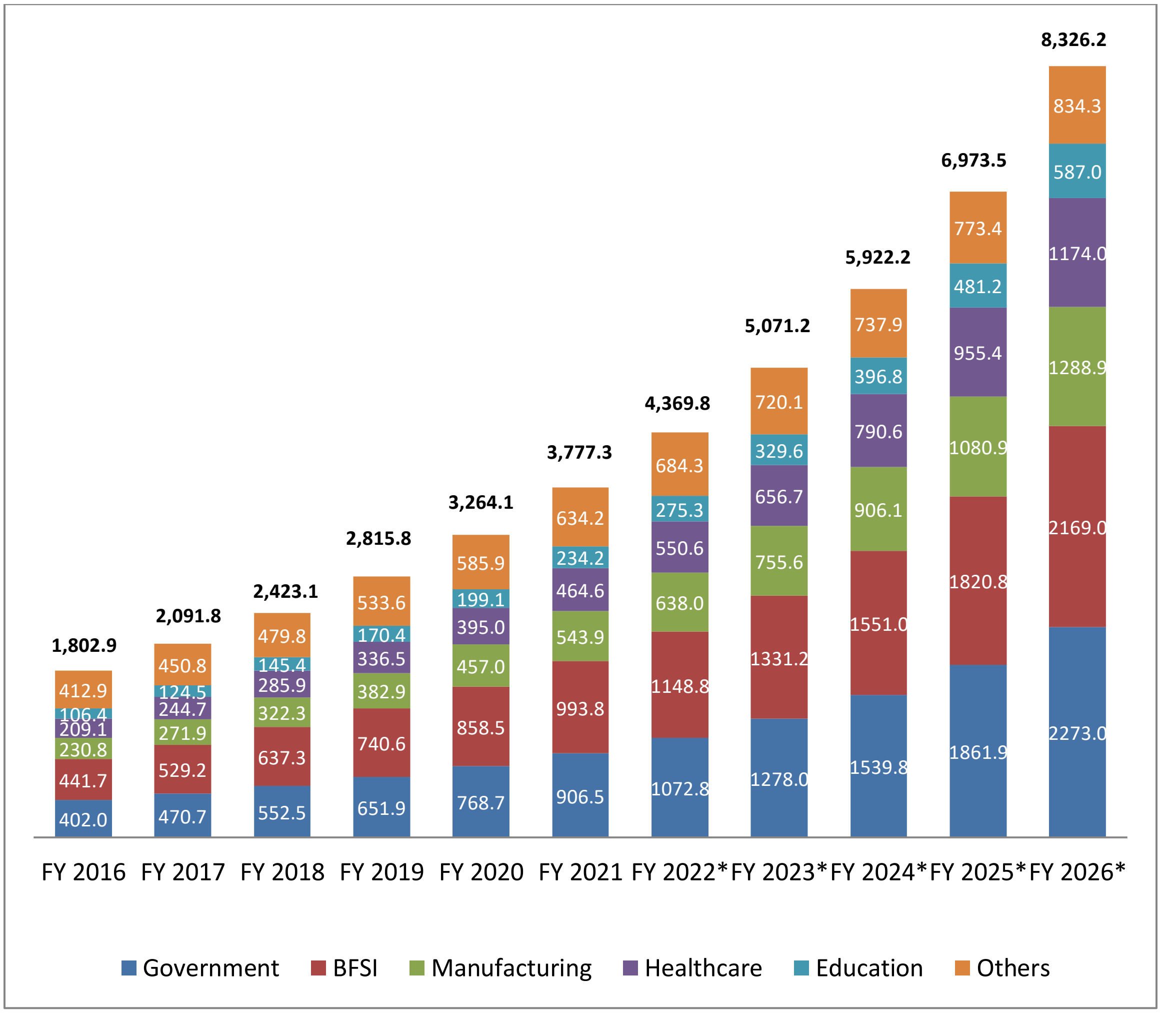
Source : Frost & Sullivan

The global players are the major stakeholders of the IoT Device Certificates market in India. This includes players like GlobalSign, Digicert, Entrust, etc. Indian companies have limited expertise in IoT device certificates with no major focus. eMudhra is aspirational in terms of investing in the market due to the high growth opportunity that lies. Since the market is still niche in India, an early mover advantage could be beneficial for eMudhra. Being a major player in the domestic Digital Certificates market, it won't be difficult for the security provider to enter into the space. IoT device certificates market is a near term market opportunity area for eMudhra.

Industry Vertical Analysis

The contribution from the Government industry vertical has become the largest in the last few years. Its revenue share has increased from 22.3% in FY 2016 to 24.0% in FY 2021 and likely to become 27.3% in the next 5 years. The various central and state government initiatives have pushed forward the demand for Digital Trust Services. DSC has strong use cases in the Government industry and is used while filing income tax return, GST, MCA e-filing, LLP registraion, customs e-filing, e-procurement, e-bidding, and e-auction. Similar strong use case of trust services are seen in the BFSI sector as well. Instead of physically visiting banks, customers can open bank accounts easily through eSign services. While doing eKYC, trust services are often used by customers. Investments on digitalization have increased in the healthcare sector which will as a whole would push forward the demand for trust services.

Figure 54: India Digital Trust Services Market by Industry Verticals – At OEM Level (INR. Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	17.7%	20.2%
BFSI	17.6%	16.9%
Manufacturing	18.7%	18.8%
Healthcare	17.3%	20.4%
Education	17.1%	20.2%
Others	9.0%	5.6%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

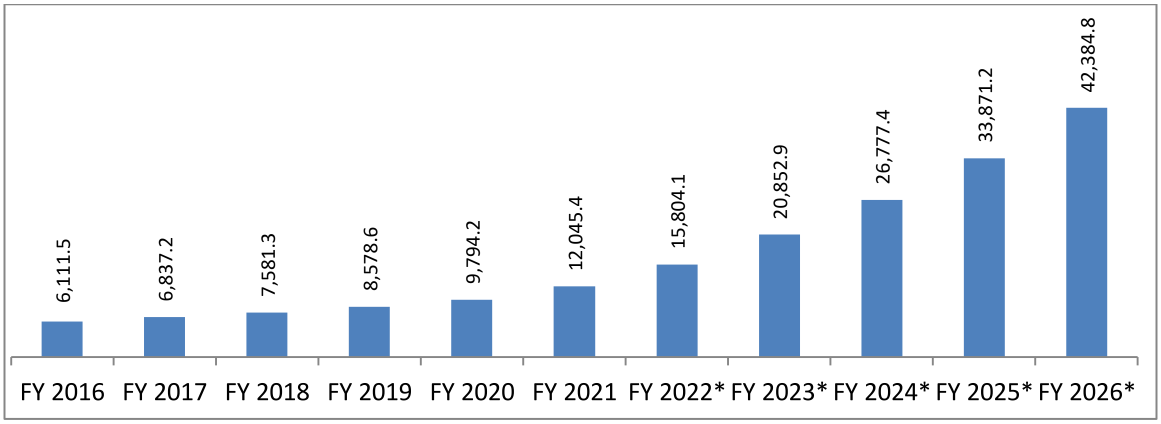
Digital Security Solutions Market

Market Size and Forecast

While the Indian government and enterprises focus on various digital initiatives, authentication and IAM remains as a fundamental area of focus. It is important that identity based frauds are minimized through the use of right authentication techniques. MFA, SSO, OTP, Digital Signatures, and biometric are few of the authentication modes prevalent in digital interfaces.

Frost & Sullivan estimates the Digital Security Solutions market which includes Authentication, IAM and PKI is currently valued at INR. 12045.4 Mn. in FY 2021 and expected to grow at CAGR of 28.6% during the forecast period. Last year, the market grew at 23.0% amidst the COVID-19 pandemic. Strong growth is expected to sustain in similar range in the next 5 years.

Figure 55: India Digital Security Solutions Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026



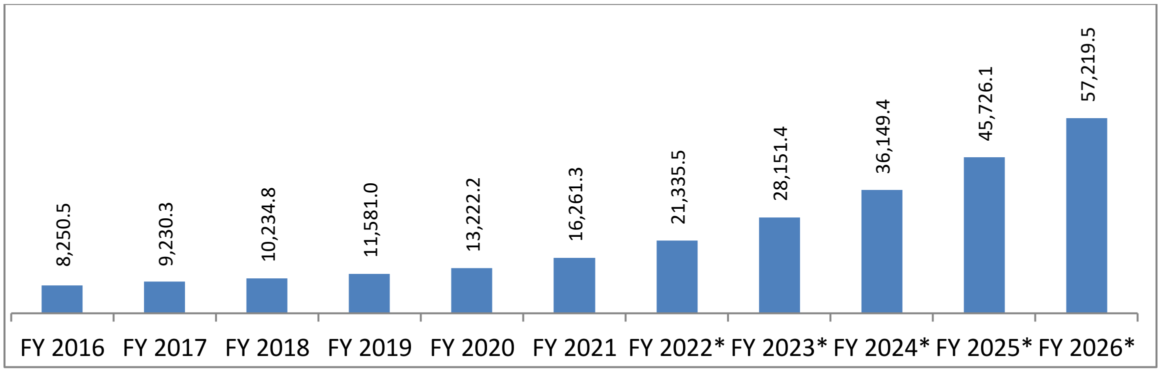
CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
14.5%	28.6%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

At the end-user level, the market is currently valued at INR. 16261.3 Mn. and expected to become INR. 57219.5 Mn. by the end of FY 2026.

Figure 56: India Digital Security Solutions Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
14.5%	28.6%

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure

Source : Frost & Sullivan

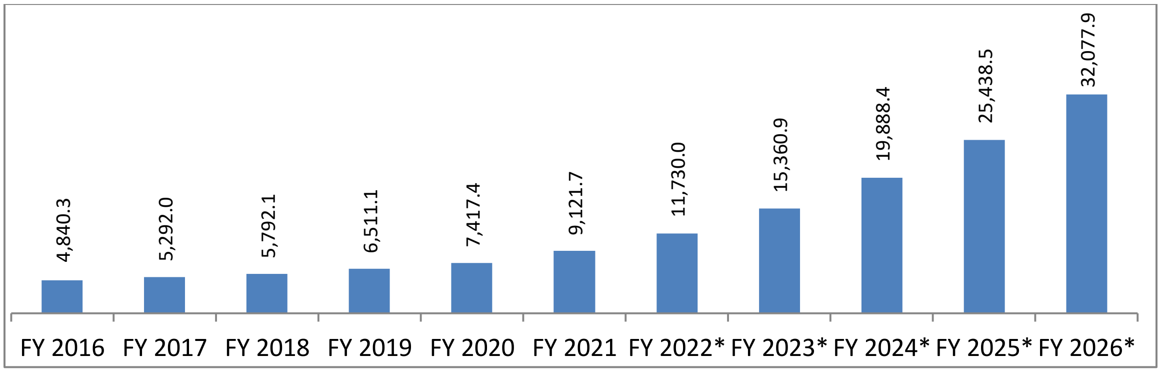
Market Size and Forecast by Digital Security Solution Applications

- **IAM Market in India**

Identity frauds have increased over the last few years. Misuse of login details and unauthorized access to database/portals has reached newer heights creating serious concerns around cybersecurity. Just depending on static passwords do not work and need MFA for improved protection. While dealing with IAM, it is important to have security solutions that provide end-to-end security, can be integrated with 3rd party applications, capabilities of scalability and high throughput processing of authentication requests and are mobile enabled. The product should be platform agnostic and accepts CA certificates for DSC and PKI based authentication.

The Indian IAM Solutions market is estimated to be INR. 9121.7 Mn. in FY 2021. The market has grown at a CAGR of 13.5% in the last 5 years. Strong growth is seen across the BFSI, IT/ITeS and Government segment. As users connect from unsecured devices, locations and networks; the need for IAM solutions has increased. Cloud is another enabler for the growth of authentication and IAM.

**Figure 57: India IAM Market – At the OEM Level (INR. Mn.),
FY 2016 – FY 2026**

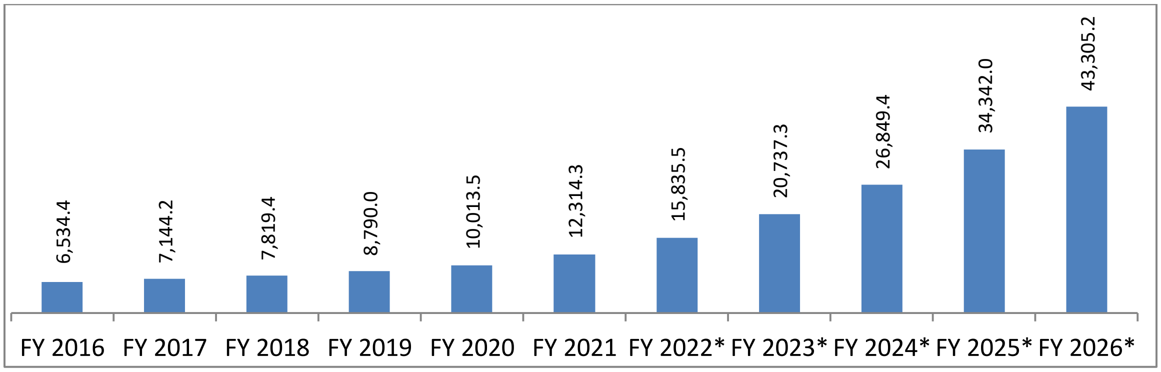


CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
13.5%	28.6%

*Projected, Base Year is FY 2021
Source : Frost & Sullivan

Much like other Digital Security products and services, channel partners who include system integrators, telcos and value added resellers sell authentication and IAM solution to Indian customers. The channel partner markup includes product implementation and integration charges. IAM projects are fairly large deals with moderate to high level of complexity.

**Figure 58: India IAM Market – At the End-user Level (INR. Mn.),
FY 2016 – FY 2026**



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
13.5%	28.6%

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure
Source : Frost & Sullivan

Competition remains aggressive in the Indian IAM market. Global players like IBM, Microsoft, Oracle, Broadcom, Ping Identity, Sailpoint, Cisco and Okta are few of the biggest names in the market. However, eMudhra is one of the major players in IAM with Indian origin. The company's emAS Identity and Access Management System is well accepted among domestic customers. emAS IAM comes with the ability to authenticate 15+ forms of authentication right up from Advanced Password and Crypto Token/Digital

Signature based authentication to Facial, Grid, Behavioral Analytics and QR Code based authentication. It supports SSO through common protocols like SAML, OAUTH, AD, LDAP with manual or auto provisioning functionality. emAS' product differentiation lies in its ability to provide adaptive or contextual security based on the risk factor (ie. location, network and device) of the user.

- **PKI Market in India**

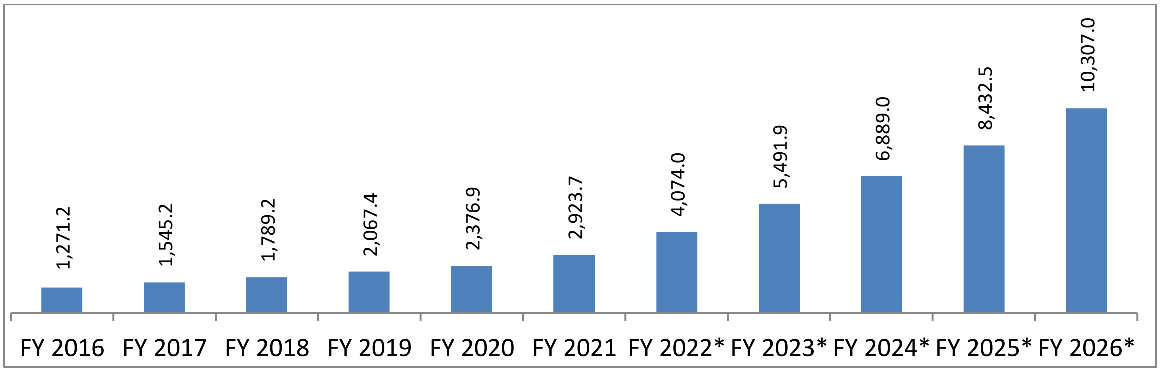
Public Key Infrastructure (PKI) is considered as the central nerve system of the digital framework. It help enterprises establish trusted signatures, encryption and identity between people, systems, and things. PKI in today's modern ecosystem is not only about securing isolated systems like email, smart cards for physical access or encrypted web traffic but is much beyond in protecting complex IT ecosystems with large number of applications, users and devices.

Use-cases of PKI

Traditional Use-case	Emerging Use-case
• SSL certificates for public-facing websites and services • Private networks and virtual private networks (VPNs) • Public cloud based applications and services • Private cloud based applications • Email security • Enterprise user authentication • Device authentication • Private cloud based authentication • Document/message signing • Code signing	• Cloud based services • Consumer mobile • Internet of Things • Consumer oriented mobile applications • BYOD policies and internal mobile device management • E-commerce

The PKI market in India was valued at INR. 2923.7 Mn. in FY 2021. Growth in the last year was recorded at 23.0%. For the next 5 years, the Indian PKI market is expected to grow at CAGR of 28.7%. The uptake of cloud and IoT is likely to push the market forward.

Figure 59: India PKI Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026

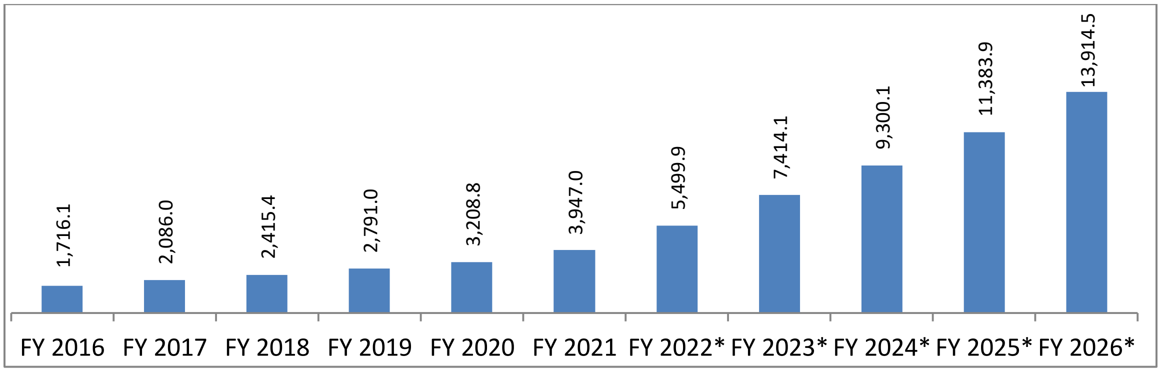


CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.1%	28.7%

*Projected, Base Year is FY 2021
Source : Frost & Sullivan

At the end-user level when PKI solutions sold to the customer, the Indian market is currently valued at INR. 3947.0 Mn.

Figure 60: India PKI Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.1%	28.7%

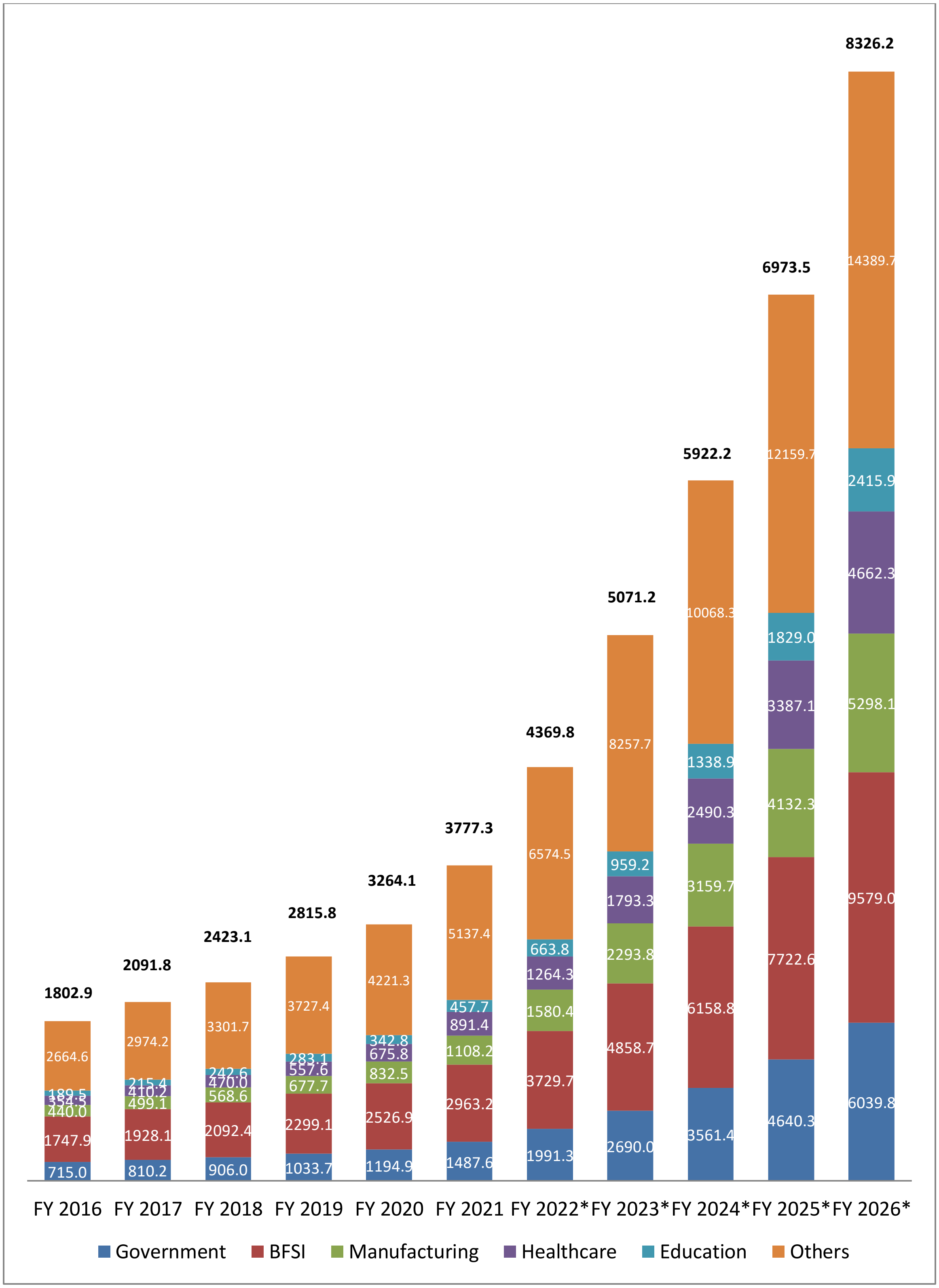
*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure
Source : Frost & Sullivan

eMudhra is one of the only Indian players who has a prominent PKI solution and competes against the global market leaders. emCA is a comprehensive end-to-end PKI digital certificate issuance and management solution that is built to provide trust, control and is robust and scalable. It has the ability to also issue certificates to smart devices in IoT ecosystem to address the emerging PKI use cases. emCA encrypts sensitive data using AES (advanced encryption standard) key that can be securely stored on HSM (hardware security module) and supports tamper proof logging. The solution offers easy migration, cost effective, can be deployed quickly and offers superior support. emCA is used in WebTrust compliant deployments. eMudhra's contribution in the PKI market could be realized from the fact that the company's Chairman V Srinivasan was appointed the Chairmanship of Asia PKI Consortium in 2019 and also as a Board Member in the Cloud Signature Consortium.

Industry Vertical Analysis

BFSI, IT-ITeS and government are the biggest users of PKI solutions. Growth in the government vertical is likely to be one among the strongest with an expected CAGR of 32.3% till FY 2026. Manufacturing, this is often termed as late adoptors of cybersecurity, are likely to embrace IAM and PKI solutions to take full advantage of digital transformation without compromsing on security.

Figure 61: India Digital Security Solutions Market by Industry Verticals – At OEM Level (INR. Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	15.8%	32.2%
BFSI	11.1%	26.4%
Manufacturing	20.3%	36.7%
Healthcare	20.3%	39.2%
Education	19.3%	39.5%
Others	14.0%	22.9%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

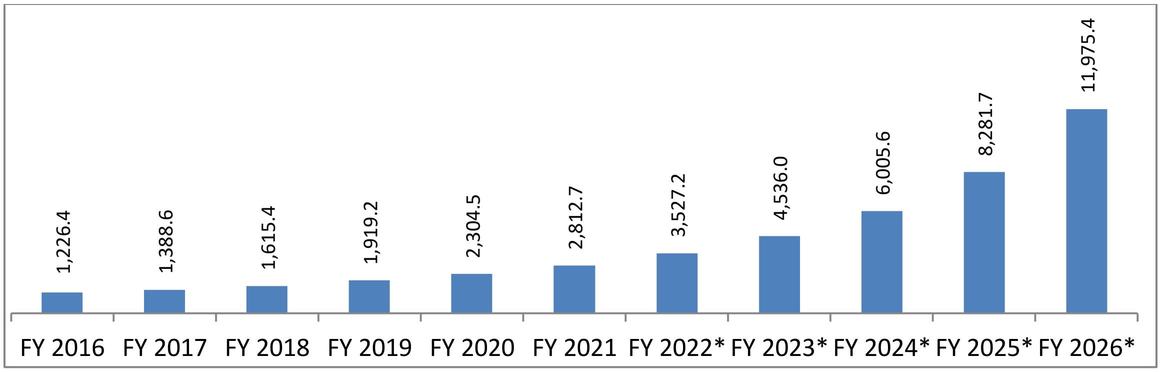
Paperless Transformation Solutions Market

Market Size and Forecast

As the concept of digital transformation picks up pace, a critical component of this is to remove the last mile hurdle of moving paper and Indian enterprises are seeking ways on how to minimize these manual interventions and replace with automation using eSignature enabled AI and ML. With paperless transformation, human efforts can be channelized to much important activities where the role of human expertise is critical. The idea of paperless transformation is not only seen in the advanced western world but also has started to make place within Indian enterprises who aim to compete strongly with their global peers. Paperless Transformation required thoughtful designing of internal and customer process and need solutions that enable these digital workflows. With the best possible eSignature enabled paperless transformation solution, customer onboarding becomes easy, invoices and contracts get signed up digitally and document sharing process become seamless. Paperless solutions are a necessary cog in the wheel for Indian enterprises in the mid to long term as they embark on their digital transformation initiatives.

Frost & Sullivan estimates the Indian Paperless Transformation solutions market to be valued at INR. 2812.7 Mn. by the end of FY 2021. Growth is likely to be near double at CAGR 33.6% for the next 5 years as against 18.1% in the last 5 years.

Figure 62: India Paperless Transformation Solutions Market – At the OEM Level (INR. Mn.), FY 2016 – FY 2026



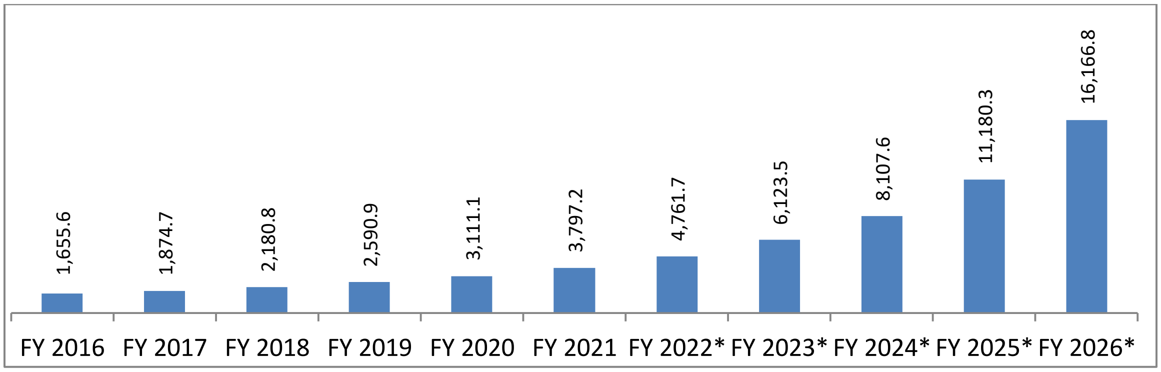
CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.1%	33.6%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

System Integrators and Digital Transformation players sell paperless transformation solutions as part of large transformation deals. It is estimated that by end of FY 2021, the Indian Paperless Transformation Solutions market was valued at INR. 3797.2 Mn. at the end user level.

Figure 63: India Paperless Transformtion Solutions Market – At the End-user Level (INR. Mn.), FY 2016 – FY 2026



CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
18.1%	33.6%

*Projected, Base Year is FY 2021, end-user revenue estimated at constant partner margin and tax structure

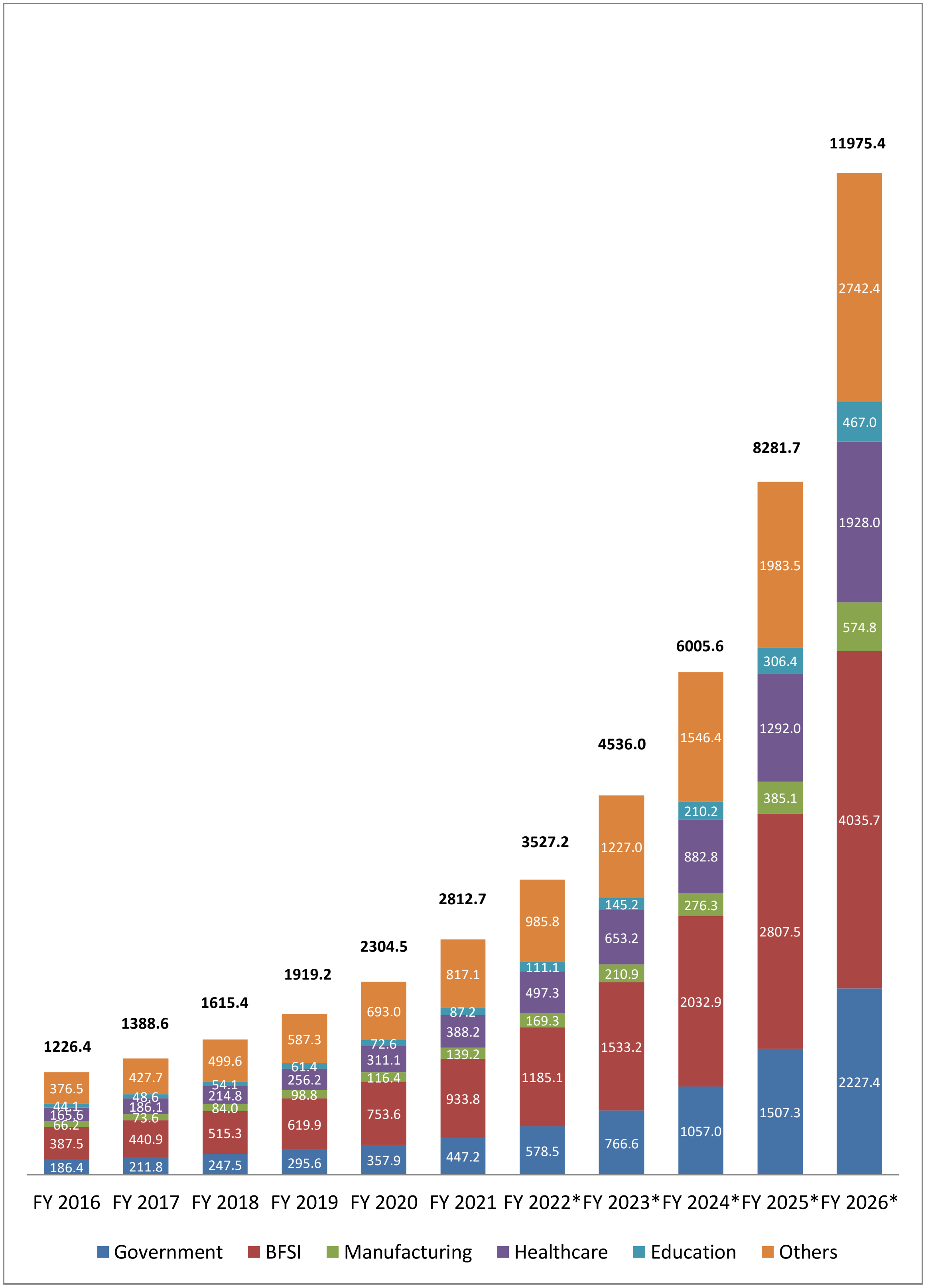
Source : Frost & Sullivan

Industry Vertical Analysis

The Paperless Transformation solutions market has strong adoption in the Indian BFSI and Government vertical. Concepts like Paperless Office help improve process efficiency and employee productivity in the BFSI sector. Customers can login to bank portals and fill in, sign and send forms digitally without the need to visit bank physically and submit forms. eSignatures and eKYC help customers sign documents digitally. Employees on the other hand can process customer requests without the need to download and manually sign documents. Paperless solutions can be synced up with ERP, CRM and other 3rd part applications to build end-to-end straight through processing capabilities. e-Bank and loan certificates can be processed and soft copies could be shared with the customer online with ease instead of sending hard copies through post.

To ease up citizen and public welfare schemes, the central and state governments have also increased focus around digitalization. In order to stop corruption, red tapism and favouratism; governments have taken up digital initiatives with presence-less and paperless mode of fulfillment. User can visit government websites and place their requests instead of standing in queues for long hours. Online status tracking is possible as the user finds the application cross various steps. Aadhaar based eSignature authentication help quicken government processes which otherwise take more time.

Figure 64: India Paperless Transformation Solutions Market by Industry Verticals – At OEM Level (INR. Mn.), FY 2016 – FY 2026



	CAGR (FY 2016 – FY 2021)	CAGR (FY 2021 – FY 2026)*
Government	19.1%	37.9%
BFSI	19.2%	34.0%
Manufacturing	16.0%	32.8%
Healthcare	18.6%	37.8%
Education	14.6%	39.9%
Others	16.8%	27.4%

*Projected, Base Year is FY 2021

Source : Frost & Sullivan

Market competition has started to grow up in the Paperless Transformation Solutions market in India. Global players like Adobe, DocuSign, and OneSpan pitch in large enterprise customers in the country. However, eMudhra remains to be one among the very few Indian companies to have started participating in RFPs targeted not only for SMBs but also for large businesses. eMudhra has been working with large Indian enterprises like Tata Steel, Infosys, Airtel, ICICI Bank, Kotak Life Insurance, etc. to claim a strong market position. In parallel, eMudhra emSigner product is being used in websites like GST, MCA, and Income Tax.

5. Overview of eMudhra Portfolio of Solutions

eMudhra is one of India's leading Digital Security and Paperless Transformation vendors. While, the company has a strong customer base in India, it has been putting in strategic efforts to expand beyond its domestic boundaries into foreign regions like Middle-East, APAC, Americas and Europe. From trust services to eSignatures, Data Security and Paperless Transformation solution; eMudhra has been working with several large and small businesses across the world to build seamless digital and paperless experiences with their clients without compromising on security by leveraging most advanced technologies in AI, ML and Automation.

eMudhra is headquartered in Bengaluru with offices spread across 7 cities in India. The company has been serving customers for the past 12 years in the area of cyber security and digital transformation. eMudhra is a 600+ member team with proprietary IP and patents. The digital transformation and security vendor has been contributing to global standards around identities and eSignatures as Board Member at Cloud Signature Consortium and Chairman of Asia PKI Consortium. The strong enterprise customers base (of 500+) are a testament of the company's excellence in solution capability, delivery, support services and most importantly - customer delight.

5.1. Value Proposition

eMudhra has been consistently designing and developing differentiated products under its various product lines – digital trust services, digital security solutions and paperless transformation – by understanding customer requirements and implementing solutions to address their challenges. Most of the products come with in-depth features and easy to infer UX (user experience) and are easily deployable. Unlike most of the other players in the market who come with cloud based solutions, eMudhra has both the versions available: on-premise and cloud; making it a vendor of choice for the highly regulated industry verticals like BFSI and government. eMudhra products are developed by adhering to various industry standards and quality levels. Over a period of time, eMudhra has built in a strong partner network which includes few of the world's largest system integrators to pitch in to government projects. The strong value proposition that the company has created for its customers make eMudhra as one of the fastest growing vendors in the space.

5.2. Solution Offerings

eMudhra is one of the very few trust service providers who operate in all the three segments of Digital Trust Services, Digital Security Solutions and Paperless Transformation solutions.

eMudhra Digital Trust Services

- **SSL/TLS Certificates**

Product	Type	Features
Domain Validation	Regular	Get HTTPS and Secure Pad Lock for Single Domain
	WildCard	Get HTTPS and Secure Pad Lock for Domain and all its

		subdomains
Organization Validation	Regular	Get HTTPS , Secure Pad Lock and Organization Validation for Single Domain
	WildCard	Get HTTPS , Secure Pad Lock and Organization Validation for Domain and all its subdomain
Extended Validation	Regular	Get HTTPS, Secure Pad Lock along with Organization Name and Country Code for the domain

- **Digital Signature Certficates**
  In accordance with the guidance issued by the Information Technology Act and the X.509 Certificate Policy for India PKI published by CCA, eMudhra issues six types of certificates: Signature, Encryption, Device, SSL Server, Code Signing and Document Signer Certificate.

  Signature Certificate: It is used by individuals or organizations for signing purpose

  Encryption Certificate: It is used by individuals or organizations to encrypt documents and retrieving whenever necessary using subscriber's private key.

  Device Certificate: This type of certificate which can be used for the purpose of device authentication in the context of IoT deployments.

  SSL Server Certificate: The SSL server certificate enables users to authenticate the server, check the validity of the web content, and establish a secure connection.

  Code Signing Certificate: It is a type of certificate which is used by software developers to digitally sign applications, drivers, executables and software programs and certifies that the code that end-users receive has not been altered or compromised by a 3rd party.

  Document Signer Certificate: This type of certificate is issued to organizational software applications for automatically signing documents/information attributed to the organization by using Digital Signature applied on the document

eMudhra Digital Security Solutions

- **emAS IAM**
  emAS IAM is the Identity and Access Management solution from eMudhra. The product comes with capabilities for Access Management and Multi Factor Authentication and Single Sign On. As a part of MFA, emAS provides enterprises the ability to authenticate with 15+ forms of authentication that includes AI based Adaptive Authentication, advanced password crypto token/digital signature based authentication among others. emAS supports SSO through common protocols like SAML, OAUTH and provisioning of users through AD/LDAP with manual

or auto provisioning functionality. One of the biggest strength of the product is advanced reporting. It supports creation and automation of many reports and extraction of historic data. The reporting module allows role based access to view or edit/create reports.

- **emCA PKI Manangement Suite**

  emCA is a comprehensive end-to-end PKI digital certificate issuance and management solution that is standards compliant, built to provide trust and control and is robust and scalable. It has the ability to also issue certificates to smart devices in IoT ecosystem to address the emerging PKI use cases. emCA encrypts sensitive data using AES (advanced encryption standard) key that can be securely stored on HSM (hardware security module) and supports tamper proof logging. The solution offers easy migration, is cost effective, can be deployed quickly and offers superior support. emCA is used in WebTrust compliant deployments (The aim of WebTrust is to promote confidence and trust between consumers and businesses on the Internet. WebTrust has formulated a series of principles and criteria designed to guide CAs to develop secured processes and policies).

  From National ID based one-time use eSign to Cloud PKI for mobility, eMudhra focuses on enabling various use cases of PKI for signing and authentication to ensure quick adoption to support digital transformation. emCA supports issuance of Digital Signature Certificates to users, servers, network devices, mobile phones, TPM (Trusted Platform Module), Trusted Execution Environment (Strong Box), IoT device, etc.

eMudhra Paperless Transformation Solutions

eMudhra's emSigner solution aims to empower enterprises with the ability to go paperless with the use of eSignatures. emSigner is an AI enabled eSignature workflow platform that powers electronic signing workflows to transform customer experience and manage risk and governance. The product is available as on-premise and cloud deployment thereby offering the choice to customers to select depending on their data residency and other compliance requirements. emSigner can be synced with major 3rd party applications like ERP and CRM to quickly sign, transfer, and check the authencity and integrity of documents generated using these platforms. The product supports 25+ languages making it easy for global customers to adopt the solution. The product is designed to offer high data security while providing multiple levels of assurance using 2-factor authentication for both internal and external signatories.

5.3. Financial Health Status

eMudhra reported a revenue of INR. 1314.97 Mn. in FY 2021. This is a growth of 13.1% from the previous year. Most of the revenue spike came from outside India (INR. 248.71 Mn. in FY 2021) with YoY growth at a whooping 72.2%. Digital Signature Certificate (CA) is the biggest revenue pocket for the company with the segment contributing over 50% of the total revenue share. In India, DSC business grew at 19.6% in FY 2021. PKI has seen a strong traction of 68.9% in the last financial year. In the global market, the PKI segment grew even stronger at 88.3% in FY 2021 (INR. 146.97 Mn.). With the strong global focus that eMudhra has decided on, the company is likely to experience even stronger growth in the next few years.

5.4. Unique Differentiation

eMudhra has the following unique differentiations as against its competitors :

- One unique Indian company with presence across all the three segments of Digital Trust Services, Digital Security Solutions and Paperless Transformation Solutions.
- Product offering across Identity, Authentication and Signing with a focus on innovation which remains key to success as the company continues to launch products based on present business needs.
- The largest licensed Cerityng Authority (CA) in India with a market share of 37.9% in Digital Signature Certificates market in India.
- One of the largest players in the Indian Digital Trust Services market with a market share of 17.8%.
- Accredited to WebTrust (only Indian company) that makes eMudhra's digital signature certificates directly recognized by browsers across the world allowing the company to issue digital signature certificates in many countries.
- One Indian company to be admitted as a member of European Cloud Signature Consortium as well as Certifying Authority / Browser Forum, a global forum that governs the use of SSL/TLS certificates.
- Only Indian company to be directly recognized by renowned browsers and document processing software companies such as like Microsoft, Mozilla, Apple and Adobe allowing eMudhra to sell digital identities to individual/organization and issue SSL/TLS certificates for website authentication, globally
- Despite being just 12 years in the market, eMudhra has better brand recognition and stronger channel partner realtionship evident from the large (500+) enterprise customer base the company has.

5.5. Industry Standards, Recognitions and Accreditions

eMudhra has added several industry recognitions over the period of time :

- One stop vendor for Digital Security and Paperless Transformation Solutions
- A ISO 9001, ISO 27001, ISO 20000-1, ISO 27018 certified company
- GDPR compliant
- HIPAA compliant
- Software development practices compliant with CMMI Level 5
- Cloud offerings compliant with SOC 2 Type 2
- Trust Services are WebTrust accredited enabling digital identity and certificate offerings globally
- Board Member of Cloud Signature Consortium and Chairman of Asia PKI Consortium
- emSigner listed in SAFE Identity Qualified Product List (QPL)
- Licensed Certifying Authority under CCA – Govt. Of India and Govt. Of Mauritius and Govt. Of UAE

- Winner of AFACT eAsia Awards 2015 (eSign product)
- One of the very few global Full Service Vendors in eSignature Workflow Management with Enterprise Delivery capability

6. Peer Group Portfolio Comparison with eMudhra

6.1. Global Players

Peer Group Profiling

- **Adobe Systems Incorporated**

  About: Adobe, originally known as Adobe Systems Incorporated, is an American computer software company with specialization in software of creation and publication of a wide range of content including graphics, photography, illustration, animation, multimedia/video, motion pictures and print.

  Products, Solutions and Services: Adobe Sign is a cloud based e-signature service that allows the user to sign, send, track, and manage signature processes using a browser or mobile device. It is part of the Adobe Document Cloud suite of services. Adobe Sign is a subscription based model sold to individuals, small business, or the enterprise. The Adobe Sign powers the e-Signature capabilities and tools inside of Adobe Acrobat Pro. Few of the capabilities of Adobe Sign include :

  - Sign forms with an electronic signature or digital signature
  - Request e-signatures
  - Upload document and send through email
  - Track and manage progress
  - Create digital forms
  - Create workflows to gather signature from multiple users

  Areas of Key Focus: Paperless Transformation Solutions

- **Entrust Corporation**

  About: Earlier known as Entrust Datacard, Entrust Corporation establishes trusted identities and conducts highly secure transactions to financial institutions, governments, corporate enterprises and other organizations. The company's diverse offerings include software to issue financial cards, produce e-passports ; authenticate users looking to access secure networks or conduct financial transactions ; provide trusted certificates for websites, mobile credentials, and connected devices ; and security modules for secure encryption and key management solutions.

  Products, Solutions and Services:

  - Certificate Solutions : includes digital certificates, digital signing, PKI and IoT Security
  - Identity and Access Management : includes Identity as a Service, Identity Enterprise, and Identity Essentials, physical/logical access, PIV compliant government mobility, privileged users, zero trust, MFA, passwordless login, adaptive authentication, SSO, APIs/SDKs
  - Data Protection : includes hardware security modules, cloud security, encryption and key management

Areas of Key Focus: SSL/TLS Certificates, Digital Signature Certificates, IoT Device Certificates, Identity and Access Management, and PKI Software

- **DigiCert Inc.**

About: DigiCert is an American technology company with offices in Australia, Ireland, Japan, India, South Africa, Switzerland and UK. It is one of the world's largest CA and trusted 3rd party and provides PKI and validation for issuing digital certificates including SSL/TLS. The SSL/TLS certificates are used to verify and authenticate the identites of organizations and domainsand to protect and data integrity of users'digital interactions with web browsers, email clients, documents, software programs, apps, networks and connected devices.

Products, Solutions and Services:

- SSL/TLS Certificates : includes Pro TLS/SSL Certificates, Business TLS/SSL Certificates, Basic TLS/SSL Certificates, Multi domain Certificates, Wildcard Certificates
- Digital Certificates : includes Verified Mark Certificates, Document Signing Certificates, Code Signing Certificates, Post Quantum Certificates, Client (S/MIME) Certificates, Secure Email Certificates (S/MIME), PSD2 Certificates, EU Qualified Certificates
- DigiCert Enterprise PKI Manager : Secure Email (S/MIME), Secure Network Access (VPN), Secure Smart Cards, Secure Devices
- DigiCert IoT Device Manager
- DigiCert Secure Software Manager
- DigiCert Document Signing Manager

Areas of Key Focus: SSL/TLS Certificates, Digital Signature Certificates, IoT Device Certificates, and PKI Certificate Discovery

- **DocuSign Inc.**

About: DocuSign is Nasdaq listed company that allow organizations to manage electronic agreements. The company offers eSignature to sign electronically on different devices. DocuSign claims to have over 1 million customers and hunderds of millions of users in more than 180 countries.

Products, Solutions and Services:

- Electronic Signature : Customers can sign and send sales contracts, offer letters and invoices from anywhere, anytime and through any device
- Contract Lifecycle Management: Streamlines the agreement lifecycle from end-to-end with DocuSign CLM. Seamlessly integrates with DocuSign eSignature and as part of the DocuSign Agreement Cloud, CLM enable enterprises to fast track the contracts and increase efficiences at scale.
- Contract Analytics : DocuSign Analyzer helps perform fast and accurate analysis of all inbound contracts to manage risk and boost staff productivity enterprise-wide
- Document Generation : Automates agreement preparation and sends for eSignature

Areas of Key Focus: Paperless Transformation Solutions (DocuSign bundles Digital Signature offering with paperless transformation/workflow and hence has been segmented under Paperless Transformation solutions)

- **Nexus Group**

  About: Part of the French IN Groupe, Nexus is a leader in innovative identity management. It develops a range of security products that form the Nexus Smart ID platform. Through its product Smart ID Solution, Nexus enable companies of all sizes and industries to issue and manage the lifecycle of trusted workforce identities and devices including IoT.

  Products, Solutions and Services:

  - Identities for Workforce: Smart ID Workforce platform
  - Identities for IoT: Smart ID IoT platform
  - Identities for Workplace Devices
  - Services: GO Workforce, GO Workplace, GO Cards, ID06, GO Authentication, GO Signing, GO IoT

  Areas of Key Focus: PKI Software

- **Sectigo**

  About: Earlier known as Comodo CA, Sectigo is a cybersecurity solutions company meant to secure websites, connected devices, applications and digital identities. It is a leading provider of digital identity solutions including SSL/TLS certificates, DevOps, IoT, and enterprise grade PKI management along with multi layered web security. One of the most popular CAs of the world, Sectigo is believed to have 700,000+ customers with an experience of over 20+ years in online trust.

  Products, Solutions and Services :

  - SSL/TLS Certificates: Single SSL Certificates, Wildcard SSL Certificates, Multi-domain SSL Certificates, DV SSL Certificates, OV SSL Certificates, EV SSL Certificates
  - Signing Certificates: S/MIME Email Encryption, Code Signing, Document Signing Certificates
  - Other Products: SiteLock Website Security, Website Backup & Recovery, eIDAS Solutions

  Areas of Key Focus: SSL/TLS Certificates, IoT Device Certificates, PKI Certificate Discovery

- **PrimeKey Solutions AB**

  About: Now part of Keyfactor, PrimeKey is an open source security software company that provide businesses and organizations worldwide with the ability to implement effective security, such as e-ID, e- Passports, authentication, digital signatures, unified digital identities and validation. Prime Key is one the world’s leading companies for cryptography and PKI solutions and has developed sucessful technologies like EJBCA Enterprise, SignServer Enterprise and PrimeKey EJBCA Appliance.

Products, Solutions and Services:

- Products : EJBCA Enterprise, SignServer Enterprise, Identity Authority Manager, SEE
- Solutions : Code Signing, PKI Migration, Document Signing, IoT and IIoT protection

Areas of Key Focus: PKI Software

Competitive Profiling

Select Players in the Global and Indian market:

	Select Players in the Global Market	Select Players in the India Market
Digital Trust Services		
SSl/TLS Certificates	DigiCert (USA), Entrust (USA), Sectigo (USA),*	DigiCert (USA), GoDaddy (USA), Entrust (USA),*
Digital Certificates	DigiCert (USA), eMudhra (India), Entrust (USA), GlobalSign (Belgium)	eMudhra (India)
IoT Certificates	DigiCert (USA), Entrust (USA), GlobalSign (Belgium),*	eMudhra (India), DigiCert (USA)
Digital Security Solutions		
IAM	IBM (USA), Microsoft (USA), Okta (USA),*	eMudhra (India), IBM (USA), Microsoft (USA)
PKI	eMudhra (India), Entrust (USA), Nexus (Sweden)	eMudhra (India), Entrust (USA), Nexus (Sweden)
Paperless Transformation Solutions	Adobe (USA), DocuSign (USA), eMudhra(India), OneSpan (USA)	Adobe (USA), DocuSign (USA), eMudhra (India)

The above mentioned table represents select players (not an exhaustive list) and denotes the company's presence in that particular segment, however does not necessarily mean that it does not have a representation in other areas of Digital Security and Paperless Transformation market

*eMudhra has built a capability and expertise around this area

Source: Frost & Sullivan

6.2. Indian Players

Peer Group Profiling (in Digital Identity, Security, and Digital Signature Certificates/CA market)

- **Capricorn Identity Services Private Ltd.**

  About: Capricorn Identity Services is one of the licensed CAs in India and issues Digital Signature Certificates to customers. The company is authorized to issue certificates to individuals, foreigners, organizations, websites, devices, etc. The company is headquarted in New Delhi, India.

  Products, Solutions and Services:

  - Solutions: includes Bulk Document Signer onUSB, Bulk Document Signer for HSM, Document Signer Certificate
  - Digital Signature Enterprise: includes PKI Components, PKI Authentication API, Signing & Encryption Components, API for DSC Enrolment, eSign.Digital

- **Verasys Technologies Private Limited (V Sign)**

  About: Verasys Technologies, incorporated in August 24, 2016 under the Companies Act, 2013 is a licensed CA in India. The company has a dedicated team of professionals who understands the domain, government rules and regulations as well as specific business need of customers and provides the best in class eSign or electronic signature related services.

  Products, Solutions and Services:

  - Products : ePDF Signer, Encrypt and Decrypt Utility, DSC
  - Services : DSC, eSign Service, Offline KYC Service, Paperless DSC

- **Sify Technologies**

  About: Sify Technologies was India's first private ISP. It is one of the Fortune 500 India company with the most comprehensive ICT service and solution. Sify's infrastructure comprises of the largest MPLS network, 10 top-of-the-lines concurrently manageable DCs, partnership with global technology majors and strong expertise in business transfomation solutions modelled on the cloud. The company has managed CA PKI service offered from its datacenter in Chennai.

  Products, Solutions and Services:

  - Digital Identity Services
  - Data Protection and Privacy Solutions
  - Transaction Security Solutions
  - Certifying Authority Setup Solution and Service
  - Authentication Solutions
  - Cryptography based Solutions

- **NSDL e-Gov Infrastructure Limited**

  About: Setup originally as a Depository in 1995, NSDL e-Gov Infrastructure Limited works closely with various government agencies for designing, managing and implementing e-Governance projects. The company uses its strengths, project management capabilities & technology expertise to deliver state of the art e-Governance solutions which help governments to identify and clear bottlenecks, promote transparency, reduce service delivery costs and deliver public services efficiently.

  NSDL e-Gov is a licensed CA in India, empanelled by Controller of Certifying Authorities (CCA) to provide eSign Services to Application Service Providers (ASPs). This is an online electronic signature service that facilitates an Aadhaar holder to digitally sign a document. An Aadhaar holder has the provision to sign a document after a biometric/OTP authentication that requires no paper based application form or document.

- **Pantagon Sign Securities Private Limited (Pantasign)**

  About: Incorporated in March 2019, Pantasign provides digital signature certificates to Indian customers. The company is committed to delivering digital signature with the highest standards. The company's portfolio of offerings primarily includes issuing DSC.

Competitive Profiling (in Digital Signature Certificates/CA market)

Licensed CAs	Class 1 -3 DSCs	eSign	SSL and Code Signing Certificates	Time Stamping
eMudhra	✓	✓	✓**	✓
Safescrypt	✓	✓		✓
IDRBT	✓ (Only to Banks)		✓* (Only to Banks)	✓ (Only to Banks)
(n)Code Solutions	✓	✓	✓*	✓
CDAC		✓		
Capricorn	✓	✓		✓
NSDL e-Gov		✓		
V Sign (Verasys)	✓	✓		
Indian Air Force	✓ (Only to IAF)			✓ (Only to IAF)
CSC		✓		
RISL (RajComp)	✓	✓	✓*	✓
Indian Army	✓ (Only to Army)		✓* (Only to Army)	✓ (Only to Army)
ID Sign	✓	✓		✓
CDSL Ventures		✓		
Pantasign	✓	✓		

*The Root CA Certificate of India is listed only in Microsoft products (including IE)

** Accredited to all leading browsers like Microsoft, Mozilla and Apple

Source : Table prepared based on the following source (https://cca.gov.in/CAServicesOverview.html), however made amendments in the column « SSL and Code Signing Certificates » based on current available information/update

7. The Way Ahead in Technology Transformation

7.1. Role of Digital Signature in Blockchain

Blockchain is one of the next-generation technologies that the world is talking about. By definition, blockchain is a shared, distributed and decentralized ledger for recording transactions, tracking assets and most importantly a trust mechanism. All transactions on a Blockchain are digitally signed so as to ensure transaction immutability and non-tamperability of data. As Blockchain systems gain adoption, Identity backed digital signatures are likely to become a critical component in ensuring traceability of parties to transactions such as Smart Contracts that get executed on Blockchain. Trust in blockchain through the usage of digital signatures also ensures that the message/information that has originated from the source and has travelled all the way to reach the destination is secured and any concerns around hacking could be ruled out.

The imperative of a Digital Signature in blockchain centers around 2 things:

- Non-repudiation : Digital Signatures ensure that the message received by the recipient has come from the sender who is believed to have sent the message
- Integrity : Digital Signatures provides assurance to the receipients about the fact that the data has not been tampered or changed while in transit

eMudhra is one of the few Indian companies positioned to tap the opportunity around digital signatures in blockchain.

7.2. Role of Digital Certificates in IoT

In the connected world, IoT devices are likely to become central to many technology products that play a critical role in our everyday lives. Embedded IoT devices collect and transfer terabytes of data over the internet everyday. From smart watches to industrial setups, IoT finds a place for itself in all fields. However, what bother users is the concern around cybersecurity in the context of IoT devices authenticating and exchanging data. Cyber criminals are always on the hunt to target the vulnerabilities on IoT devices and compromise them to launch massive attacks. Typical attacks on the IoT devices includes DDoS, PDoS, Spamming, MITM, RFID Skimming, and more. IoT devices with default passwords are often the easy target for miscreants. Legacy security techniques fail to provide the best possible security for IoT devices and hence need advanced technologies for fool proof protection.

With the advent and popularity of digital technologies, digital signatures certificates issued to devices are likely to become an integral part of IoT systems to restrict illegal users. Device certificates embedded in IoT devices allow devices to identity and authenticate themselves as part of the IoT network. Further, using digital signature certificates data sent over public/private networks can be signed and encrypted to ensure data integrity and confidentiality. Software developers are resorting to code signing in the software release process to ensure integrity of the IoT device software and firmware updates and to defend against risks connected to code tampering or code change. In public key cryptography, code signing is the specific use of digital signatures that help organizations to identity of the software developer and ensures/certifies that the software has not been tampered/changed after it has been released. Moving ahead, digital signatures certificates are likely to become central to ensure security of IoT ecosystems.

7.3. Role of Digital Signature Certificates in Quantum Computing

Enterprises are fast becoming aware of the fact that quatum computers will make existing encryption techniques obsolete. The future is quantum safe algorithms which is likely to pick up very soon. In July 2020, NIST (National Institute of Standards and Technology) announced the completion of second round in its selection of quantum-safe crypto algorithms. From 69 submissions received (from various cryptographic experts around the world), NIST has narrowed down to 15. The 3rd round has begun and this selection round would help NIST to decide on the first post-quantum cryptography standard. The 3rd round is expected to be complete by 2022. Once the final algorithms are finalized, it will be important for enterprises to discover and categorize the full set of certificates in use, replace them with quantum safe algorithms and implement automated certificate management solutions to manage this rollout effectively. This will present an opportunity for vendors to design solutions that support deployment of quantum-safe cryptography and benefit from adoption of quantum computing in the future.