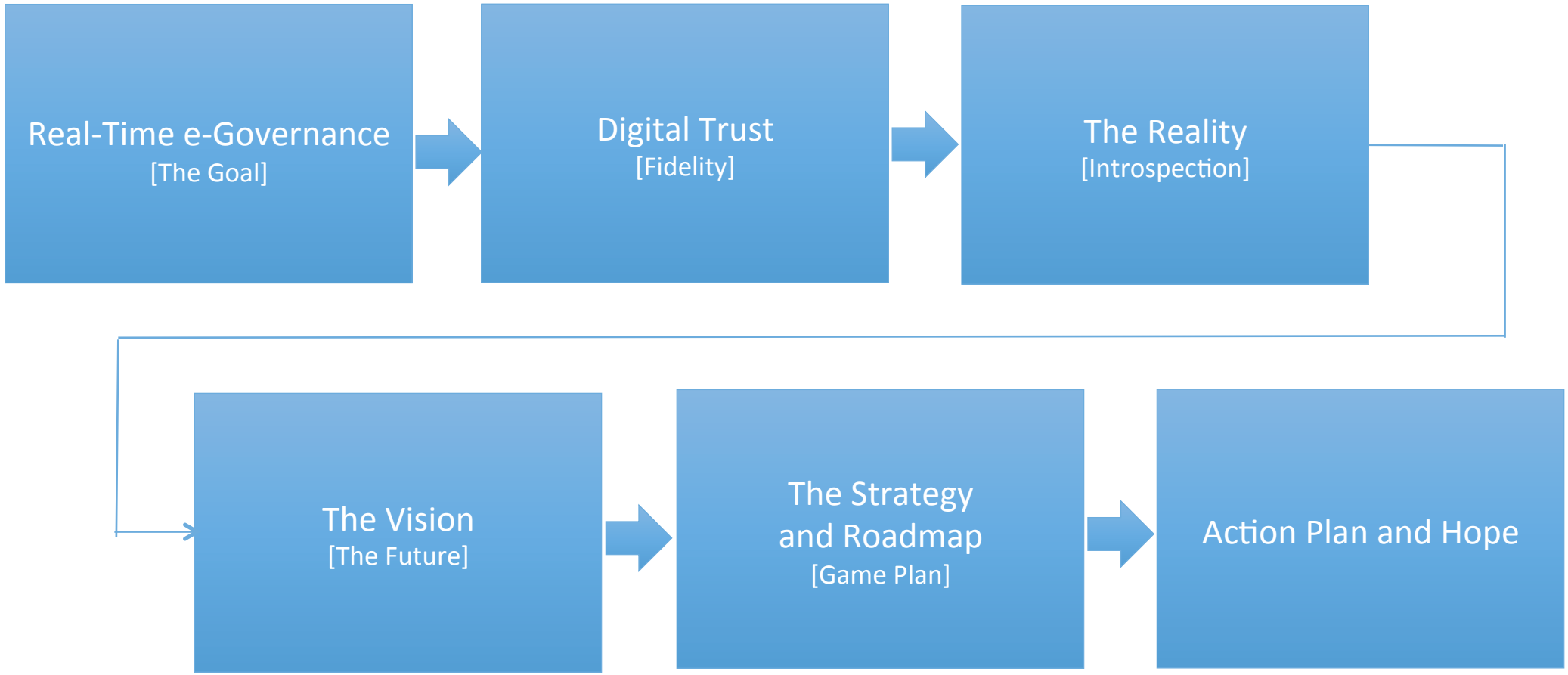
FORTYTWO42
Bringing ideas to life

Towards a (Secure ? !) Digital Nation

Vision, Strategy and Roadmap

Sanjay Deshpande
Managing Partner & Chief Scientist
FortyTwo42 Labs
Date: 9th January 2017

The Structure



Key Global Initiatives in Secure Digital Transformations

- **United Kingdom**: Time bound programs launched for Secure Smart Cities and FINTECH innovations
- **India**: Massive push for Digital Financial Ecosystem and Real-Time e-Governance
- **Switzerland:** Swisscom Secure IOT network
- **South Korea**: Deployment of ubiquitous sensor network dedicated for IOT driven public services
- **Germany:** National prioritization for Industry 4.0

Towards a (Secure?) “Digital National”

Next Generation Strategy for Economic Growth, Governance and Policy Execution

FORTYTWO42
Bringing ideas to life

Government's Role in Accelerating Economic Growth

Make economic environment conducive for **innovation**

Institution building, public skill development and training

Efficient, equal, transparent, **services delivery to all citizens**

Create **open debate** about acceptability of new systems, particularly related to **privacy, safety, security, and resilience**

Create and support dynamic, **competitive market**

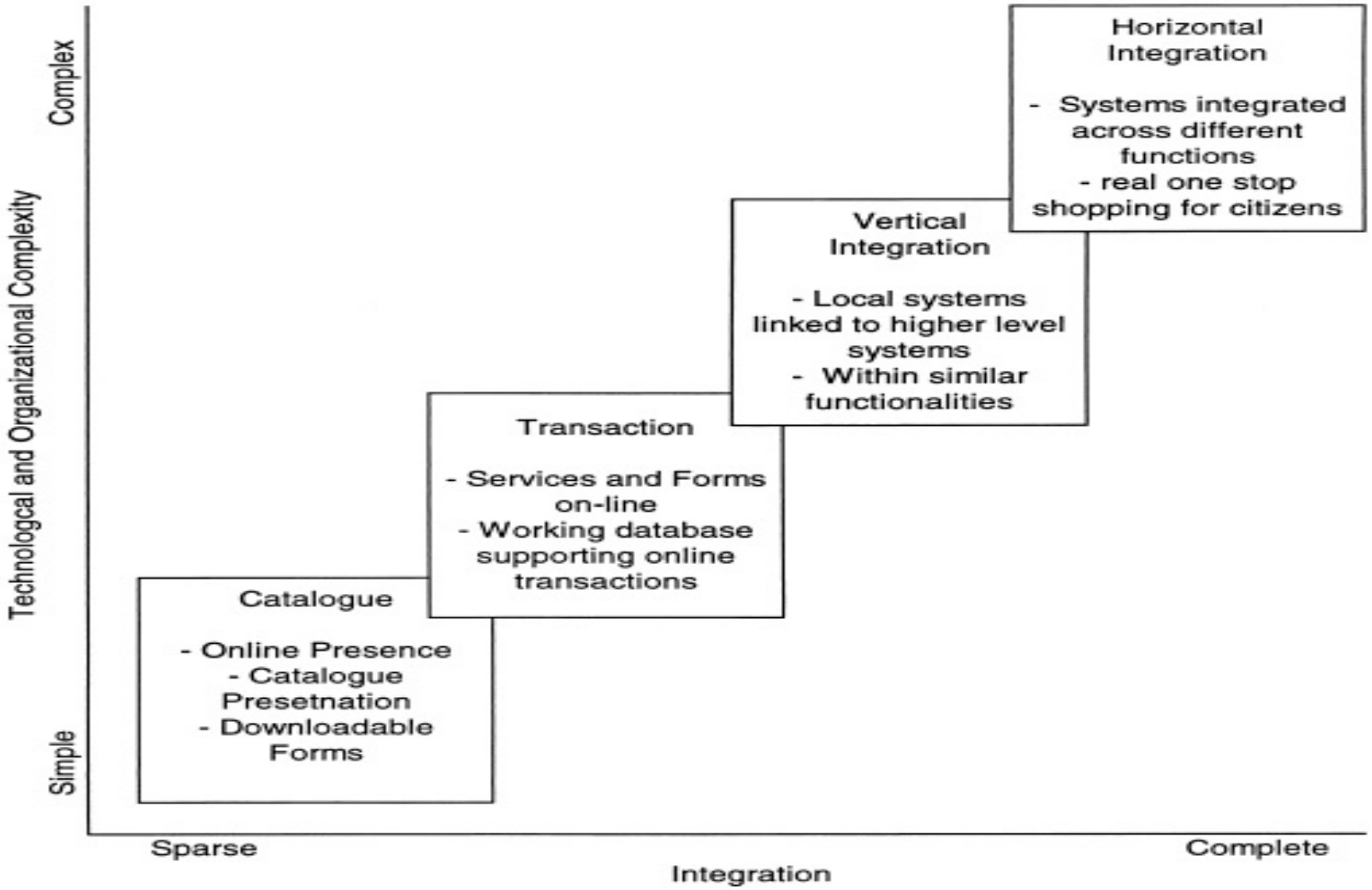
The DIGITAL INDIA VISION

Prime Minister Shri Narendra Modi launched the Digital India program with a vision "**to transform India into a digitally empowered society and knowledge economy**"

Core Areas

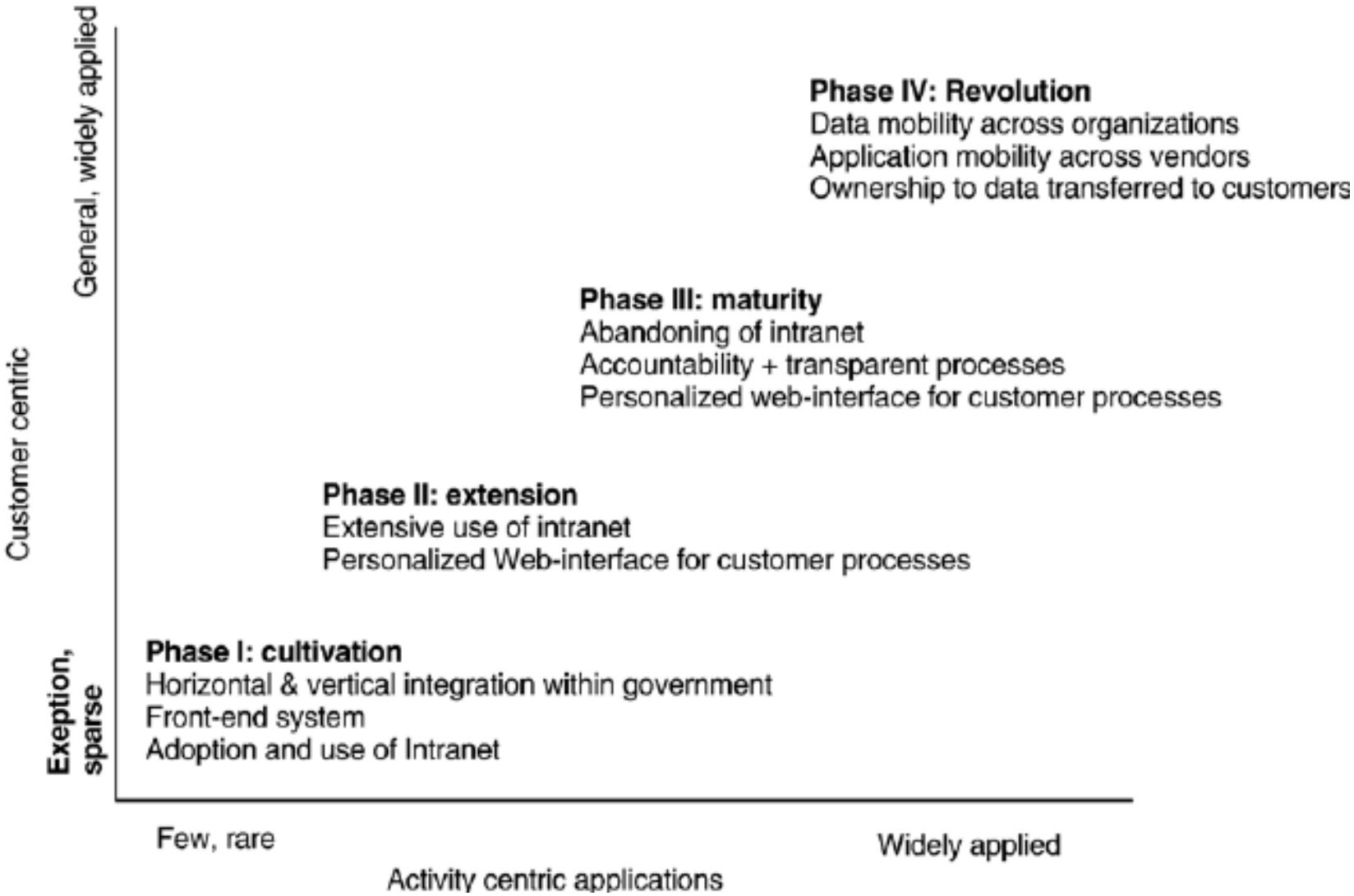
- Digital infrastructure as a utility to every citizen
- Governance & services on demand
- Digital empowerment of citizens
- Digital economy
- Cyber-physical engagement

eGovernment Maturity Model: Type 1



Ref: Layne and Lee Model of e-Governance

e-Government Maturity Model: Type 2



Ref: Andersen and Henriksen

Fidelity of Real-Time eGovernance

Transforming eGovernance to **Real-Time eGovernance**

@ the Speed of "?" : Citizens are a very impatient lot

Fidelity of eGovernance and its fundamental role

What about **Digital Trust** and how to achieve it?

IF WE DON’T FIX AND INSTALL A **NATIONAL CYBER SECURITY INFRASTRUCTURE …**
WITH A MISSION MODE PRIORITY….
….WE ARE HEADING FOR A MASSIVE DISRUPTION IN ECONOMIC GROWTH.

PERIOD.

DIGITAL TRUST

Why, What and How?

What is Digital Trust?

Real-Time eGovernance needs to ensure fidelity of their digital transactions, while delivering digital services across various channels to its users ***in order to prevent cyber fraud***.

Delivering Transaction Fidelity with a Single Unified Technology. Seamlessly.

All the transacting parties are authenticated	Transaction details are private	Transaction is authorized & verified	Transaction is not modified/tampered later	Transacting Parties cannot deny the transaction in the future
				
Multi-Party IDENTITY & AUTHENTICATION	**Dynamic Key Data ENCRYPTION**	**Workflow based AUTHORIZATION & VERIFICATION**	**Embedded DATA INTEGRITY**	**In-Line Transaction Siging NON REPUDIATION**

The Reality

Introspection

Current Threat Landscape

- The end **users of the e-Government infrastructure remain vulnerable to variety of threats** such as Packet Sniffing, Probe, Malware, Internet Infrastructure Attacks, Denial of Service (DOS) Attack, Remote to Local (R2L) Attack, User to Root (U2R) Attack

- **Data theft**, **financial/digital transaction attacks**, corruption of data, **defacement**, extortion, cyber bullying, intellectual property theft, business espionage.

- Governmental institutes and critical infrastructures bear significant weight in the amount of attacks they encounter.

- An attacker may have **political**, **economic**, **military**, **intellectual** and **financial aims.**

- **Most high impact attacks are now orchestrated by nation state**s.

Current Innovation Scenario

We import most of the cyber security technologies from rest of the world

There are no incentive structures for building indigenous cutting edge next generation cyber security technologies

A national priority on creating a robust cyber security infrastructure is fundamentally missing

A culture of innovation and leadership in building both defence and "attack for defence" platforms is dormant inspite of the availability of vast amount of talent and capital

We work in silos and groups (while the hackers work collectively as one virtual unit)

Current Technology Scenario

Lack of End-to-End Identity, Authorization and Control Workflow

Cost and Complexity of Security

Static Security Posture

Poor Usability

Lower Adoption

The Vision:

Secure Hi-Fidelity Real-Time eGovernance

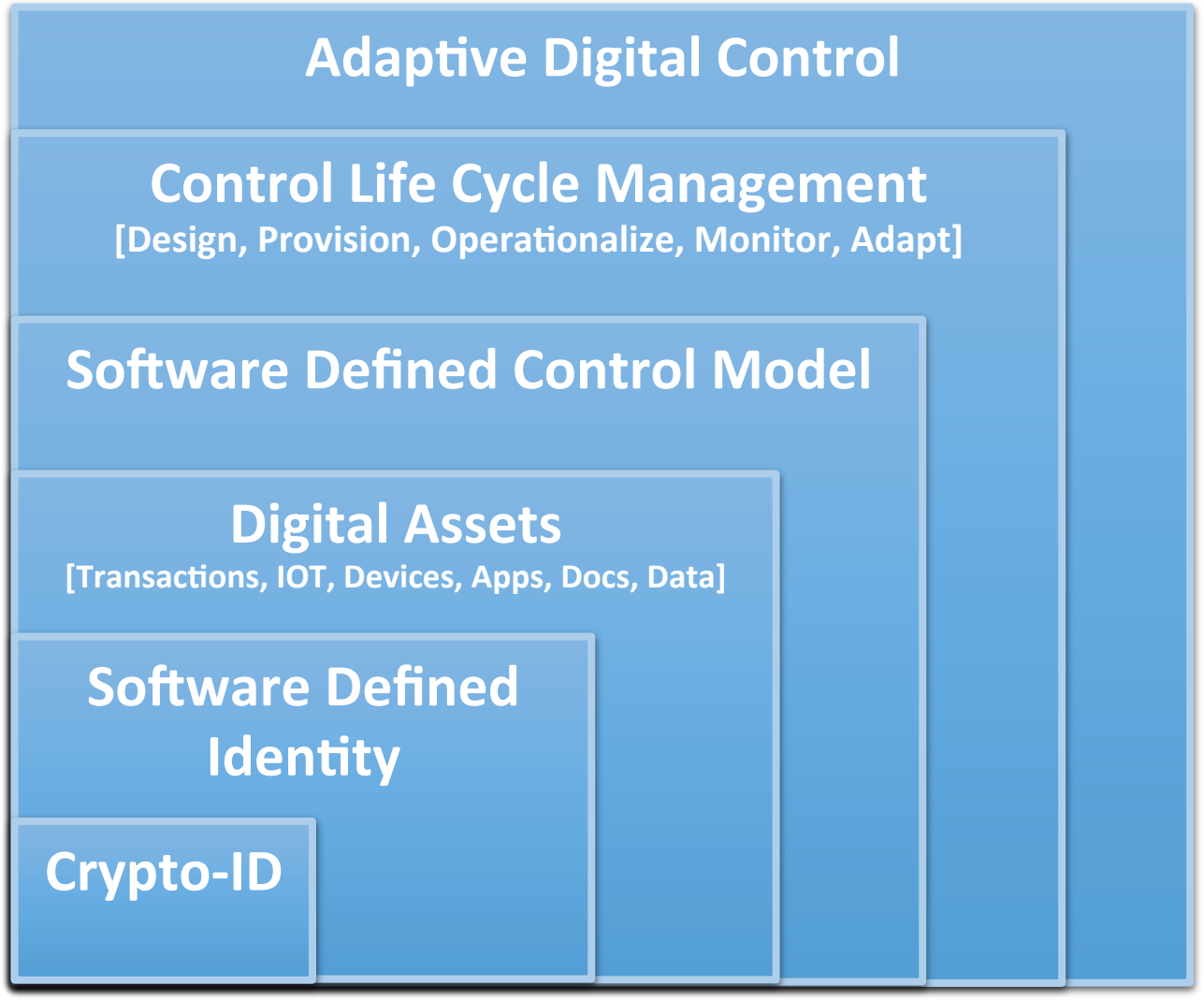
Leading the World through Cutting Edge Innovation in Secure Computing and Communications

THE VISION

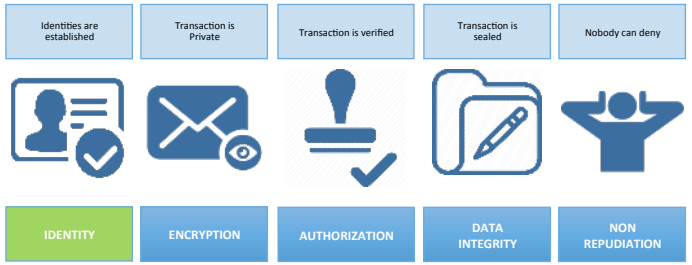
To create a **world-class secure and safe real-time eGovernance "ecosystem"** that is **built on top of a future proof, dynamic and evolving national cyber security infrastructure to protect the Citizens, the Financial, Industrial Ecosystem and Indian Defence** from external and internal **cyber threats** to rapidly **accelerate the economic growth of the country.**

Technology Vision : Towards Adaptive Security Control

Software defined automated, machine learning adaptive agile security control platform.



THE IDENTITY



IDVx
I-AM™ Identity Verification Index

User IDs
Google, Facebook, Mobile Number

Government IDs
Aadhaar, Passport, PAN

Cryptographic Identity

Enterprise IDs
Account Number, Internet Banking User ID

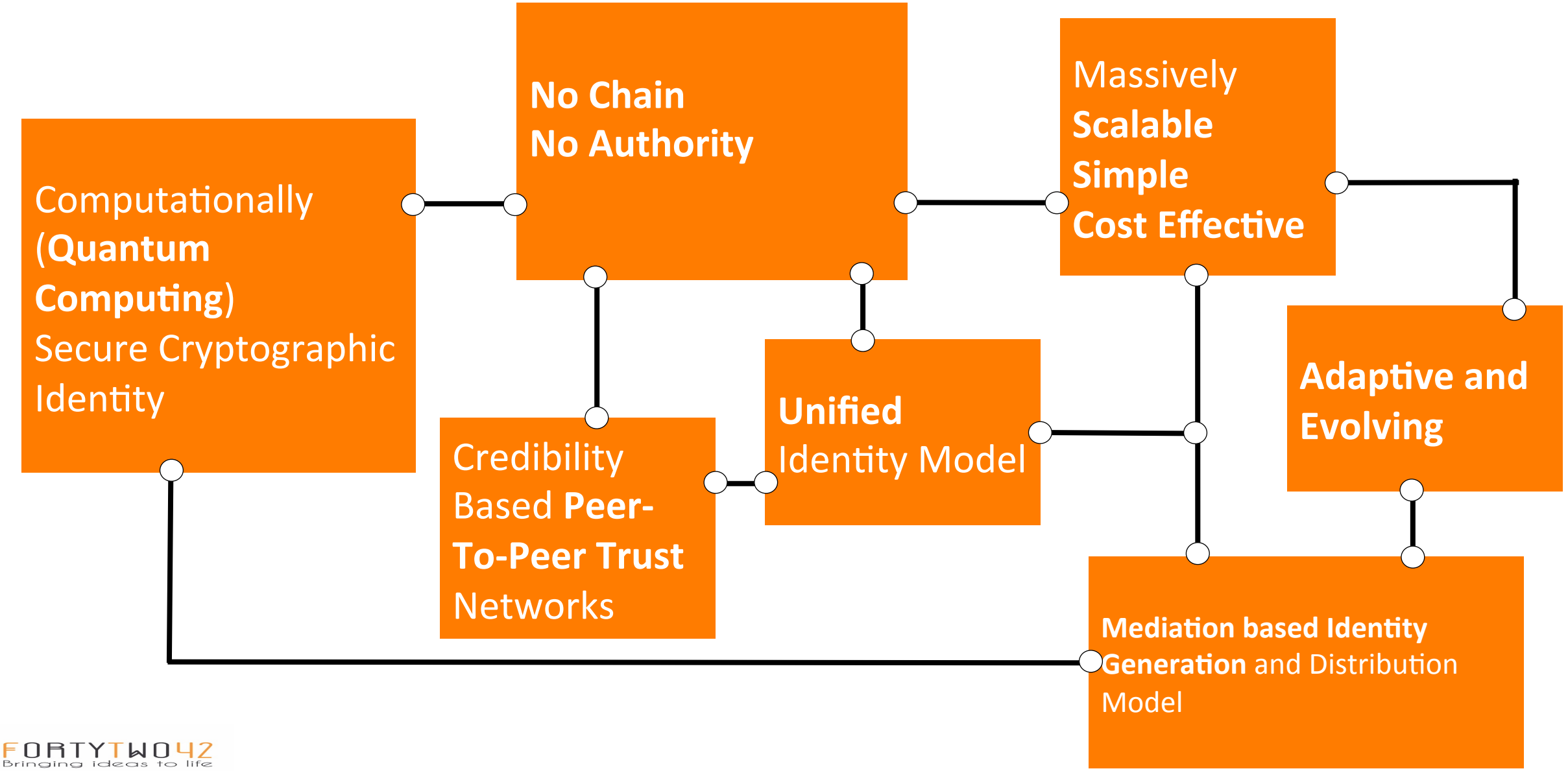
Users/ Enterprises/ Things
[Identity Chaining]

Unifies End-User Identities
Enables Identity Chaining
Dynamic Configurable Verification Index
PKI Grade Crypto Strength

A Non-PKI Digital World::[An Example of Disruptive Innovation]

@ FortyTwo Labs in Vizag

BEYOND PKI



FORTYTWO42
Bringing ideas to life

The Strategy and Roadmap

A (time bound!) Execution

#1 End-to-End Integrated Adaptive Holistic Security Control Ecosystem

#2 Components of a Holistic End-To-End National Cyber Security Ecosystem

- **Collaborative Model**
- **Securing the entire inter-connected chain**
- **Cyber Warfare Readiness and Anti-Terrorism**
- **Integrated Real-Time CERT and Cyber Threat Intelligence**
- **Indigenous Prevention/Defense/Attack Solutions**
- **Best in Class Global detection solutions & SIEM/ SOC**
- **Incident Response (Tools, Processes, Skills and Values)**
- **Business Continuity and Disaster Recovery**
- **Physical Security**

#3 Securing the National Digital Infrastructure : A Four Step Process

- **Step 1: Map all the critical national digital (and sometimes non-digital) assets vis-à-vis the threat vectors**. This might include security procedures, data stores, network architecture, physical offices, central servers, portable devices.

- **Step 2: Conduct a detailed/comprehensive national level threat landscape survey** - this analysis will help create a coherent risk map that enables controls, and security measures to be put into place in an intelligent manner while taking into consideration the true nature of the exposure.

- **Step 3**: **Identify all the contours/perimeters of defense/attack –** this analysis should cover all the users, devices, applications, servers, network, and data center (hardware and software).

- **Step 4**: **Define**, **Provision and Enforce Policies and relevant security technologies** for each of the assets in the contours in relation to the cyber threats

#4 Design and Deploy Holistic End-To End Security Controls

- User Identity and Authentication Policies/ Technologies
- Device/IOT Authentication Policy
- Data Encryption Standards
- Application Development Process
- Data Center Access Policies
- Application and Device Access policy
- Continuous Threat Monitoring
- Business continuity technologies and policies.
- Identity and Access management policies and infrastructure.
- Privileged access control policies and data breach/leakage detection and control

#5 National and State Level Real Time Cyber Security Threat Index

- **National Cyber Security Threat index should be defined and computed** in real-time and communicated to all the concerned stakeholders.

- **Such an index (like the stock market) will provide the current "temperature" of the cyber threat to all the concerned stakeholders in real-time for them to activate the required response strategies** in real-time thereby drastically reducing the threat response reaction times.

- **The National/State Level Cyber Security Index is a real-time measure of the risk to the corporate, industrial, and governmental information infrastructure from a spectrum of cyber security threats.**

- **It is based both on the sentiment as well as real time data collected on the cyber threats from across the ecosystem** in recognition of the rapid change in cyber security threats and postures, the state of cyber security metrics as a practical art, and the degree of uncertainty in any risk-centered field.

#6 Cyber Security Maturity Model for eGovernance Ecosystem (**CSM2 for eGov**)

- **Cyber Security Maturity Model** will enable the state to measure the cyber security maturity level vis-à-vis a standard model.
- These models **can be customized for various digital entities** within the cyber security ecosystem – citizens, enterprises, government departments and critical infrastructure.
- The overall **national cyber security maturity level** can be modeled as an integration of these individual sub-models.
- **The state can further enforce/recommend compliance by citizens, enterprises, government departments in accordance to this maturity model**.

7 Create World Class Cyber Security Clusters

Cyber Security Cluster is

- **a network of dedicated cyber and info security specialists, investors, start-ups, academia, research institutes, private labs coming together in groups**

- **who actively work to create unique solutions and build IP for e-Governance, national critical infrastructure security and other commercial cyber security technologies.**

7 Create World Class Cyber Security Clusters

- These Cyber security clusters will act as a catalyst to support the members of the cluster by communicating strategic initiatives critical to state e-Governance implementation

- They will provide a networking platform to share ideas and best practice, can find new ways to grow and spur innovation and technology IP creation in the field of cyber security.

- Specialist cyber security companies, labs, R&D centers will build cyber security knowledge, skills, and capabilities in the region, to make businesses more resilient to cyber-attacks.

- AP Govt's fast and collaborative approach enables and places AP Govt. to be a leader in the field of cyber security. Vizag has already launched India's first Cyber Security and FINTECH cluster.

7 Create Frameworks and Policies for Secure IOT Infrastructure for Secure Smart Cities, Real-Time Sensor Data Networks for Agriculture and Home Land Security

- Institutionalize and provision a policy for securing IOT infrastructure to ensure the safety of the cyber-physical world
- Set-up state and national Level R&D Centers in a PPP model to develop new security models and technologies will be required to be innovated
- Identify critical infrastructure (smart cities, survey data, agriculture data, home land security/drones/ surveillance) and secure them on highest priority in a time-bound manner

Way Forward

The VIZAG Cyber Security Cluster

Trust in government is one of the most precious state assets. Public support can help mobilize ambitious and innovative government policies.

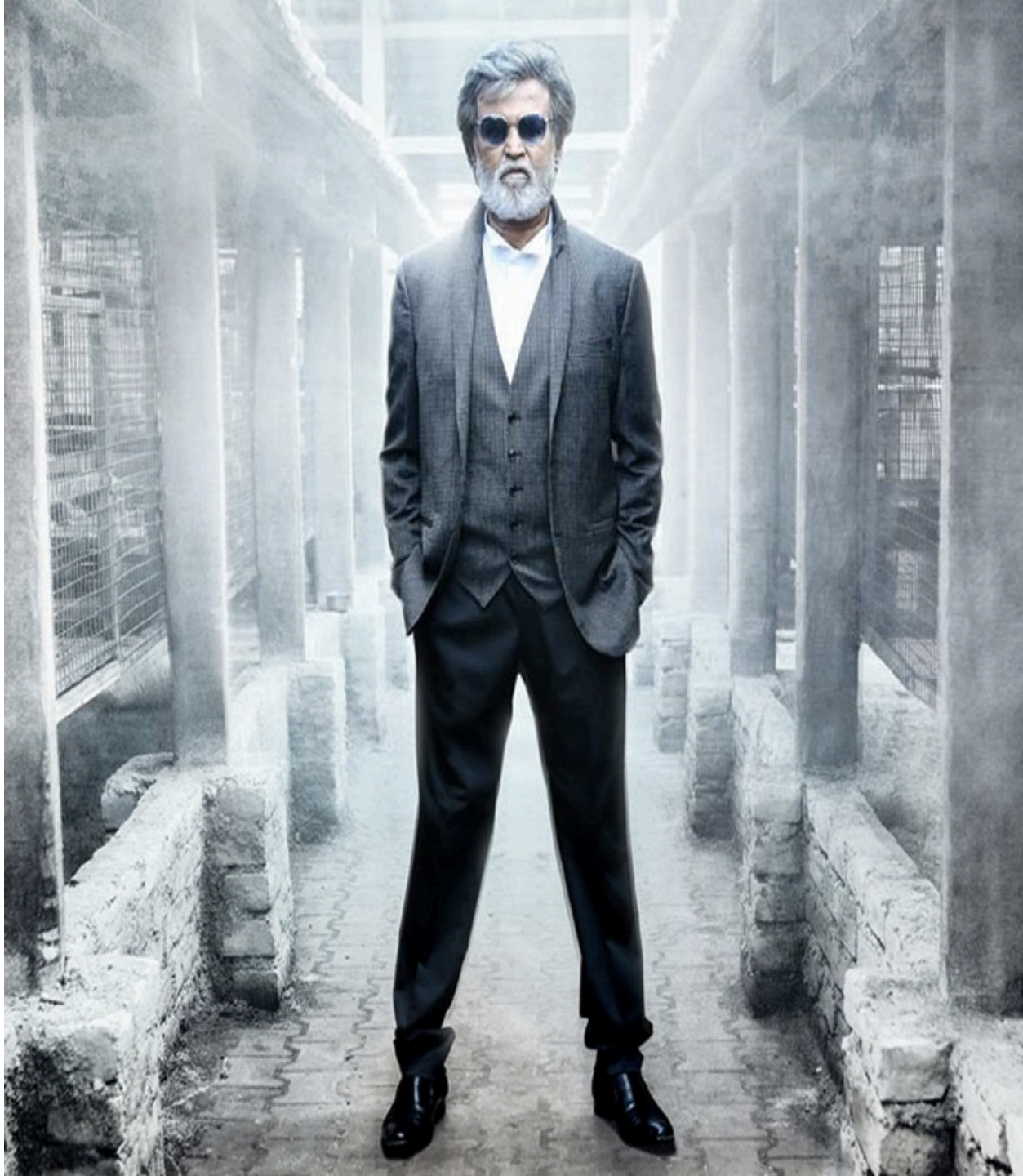
Necessary cyber security measures must be incorporated by design into the system.

A holistic cyber security infrastructure is the fundamental building block on top of which safe and secure Real Time e-Governance delivery systems can be built

AP State and Vizag is well poised to **lead the country and the world.**

In order to fulfill this vision **the state leadership will have to prioritize and allocate the necessary budgets, and execute the critical cyber security related initiatives in a time bound and mission mode.**

We should aim to be bold, courageous, and innovative



FORTYTWO42
Bringing ideas to life

@ VIZAG

India's First
Cyber Security and
Fintech Cluster with an
Amazing Beach !

SANJAY@FORTYTWO42.IN