From eID to Identity Services Infrastructure - Practical implementations for sustainable success

Jon Shamah
EMEA Sales Director
CoreStreet Limited

Card-Ex 2006, CICC

Agenda

- About CoreStreet
- Vision
  - ID Validation & Applications
  - Societal Infrastructure
- Implementation
  - Identity Services Infrastructure (ISI) introduction – a comprehensive approach to a sustainable National Identity Program
  - Distributed Validation & Authorization
  - Identity Services Infrastructure Components
  - Case study: Multi-million user government deployment

CoreStreet

About CoreStreet

What We Make:	Massively scalable, secure and survivable electronic credential validating software
Founded:	October 2001 – roots in MIT Dept of Cryptography
Employees:	50
Headquarters:	Cambridge, MA, United States
IP:	15 issued patents + 18 filed patents
Target Markets:	Population Scale eID, - Government, Defence, Corporate

CoreStreet

Differentiating Usage

- **National ID**
  - Interaction between State and Citizen
  - Low value to Citizen

- **eID**
  - Interaction between Citizen and Citizen or Business
  - High value to Citizen

Often co-incident and the same ID credential

CoreStreet

Same Two Basic Questions

- **Authentication**
  - Are you who you say you are?
    - PIN
    - Biometrics
- **Validation & Authorization**
  - What are you allowed to do?
    - Revocation
    - Attributes/privileges

CoreStreet

Validation & Authorization Example: Driving License

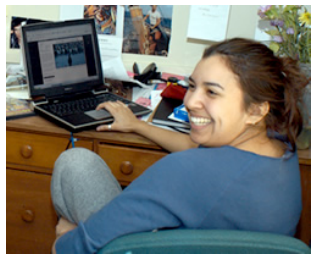
- **The driver is suspended from driving because of a number of traffic offences**
  - The licence does not reflect any recent changes to the driver's status to drive. It may not be possible to confiscate the license.

- **The police officer can confirm that the licence belongs to the driver, but how can he determine if the holder of the license is currently permitted to drive a car?**

Or if the driver has outstanding arrest warrants…

Or if the driver is known to be dangerous

Thinking Beyond Issuance



Different activities require differing levels of validation

CoreStreet

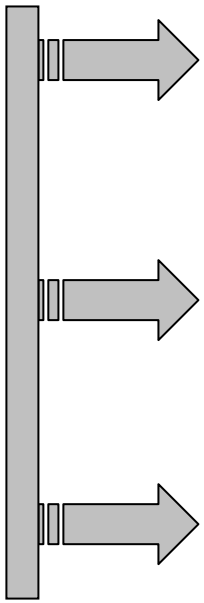
Key Principle:

Separate long lived identity information

from privileges

One Identity - One Card …… the potential for many privileges

Key Principle – Separate Long Lived Identity Information From Privileges



High security ID control

- E-passports – e-visa
- National / Resident ID card
- Military ID badge
- eAccess Gate
  - Border Crossing
  - Event admission

Fraud & Cost Reduction

- Car registration
- Driving license
- Social benefit card
- Health card
- Student card
- Migrant Worker Card

New services to citizen /corporation

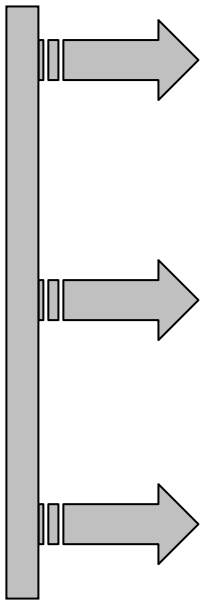
- Digital Family Registry
- Government portal access
- Electronic polling system
- City cards - Transportation
- Tax Tele-declaration
- 3rd Party Identity Validation Services

Examples of Potential Privileges

CoreStreet

One Identity - One Card …… the potential for many privileges

Key Principle – Separate Long Lived Identity Information From Privileges



High security ID control

- E-passports – e-visa
- National / Resident ID card
- Military ID badge
- eAccess Gate
  - Border Crossing
  - Event admission

Fraud & Cost Reduction

- Car registration
- Driving license
- Social benefit card
- Health card
- Student card
- Migrant Worker Card

New services to citizen /corporation

- Digital Family Registry
- Government portal access
- Electronic polling system
- City cards - Transportation
- Tax Tele-declaration
- 3rd Party Identity Validation Services

Examples of Potential Privileges

CoreStreet

One Identity - One Card …… the potential for many privileges

Key Principle – Separate Long Lived Identity Information From Privileges

High security ID control

- E-passports – e-visa
- National / Resident ID card
- Military ID badge
- eAccess Gate
  - Border Crossing
  - Event admission

Fraud & Cost Reduction

- Car registration
- Driving license
- Social benefit card
- Health card
- Student card
- Migrant Worker Card

New services to citizen /corporation

- Digital Family Registry
- Government portal access
- Electronic polling system
- City cards - Transportation
- Tax Tele-declaration
- 3rd Party Identity Validation Services

Examples of Potential Privileges

CoreStreet

One Identity - One Card …… the potential for many privileges

Key Principle – Separate Long Lived Identity Information From Privileges

High security ID control

- E-passports – e-visa
- National / Resident ID card
- Military ID badge
- eAccess Gate
  - Border Crossing
  - Event admission

Fraud & Cost Reduction

- Car registration
- Driving license
- Social benefit card
- Health card
- Student card
- Migrant Worker Card

New services to citizen /corporation

- **Digital Family Registry**
- **Government portal access**
- **Electronic polling system**
- **City cards - Transportation**
- **Tax Tele-declaration**
- **3rd Party Identity Validation Services**

Examples of Potential Privileges

CoreStreet

Identity Validation – Different Activities

- **Different activities require different levels of authentication**
  - Signing
  - Auditing
  - Remote Identity verification
  - Local (one-to-one) identity verification
- **Levels dependent on risk environment & liability**
  - Financial transactions
    - Underwritten by institutions or insurers
  - Informational transactions
    - Compliance
    - Security
    - Harder to quantify loss and so harder to offset

CoreStreet

Planning for Success

- **The acceptance and widespread use of eID will cause a massive increase in validations of all levels and will quickly overwhelm first generation technologies.**

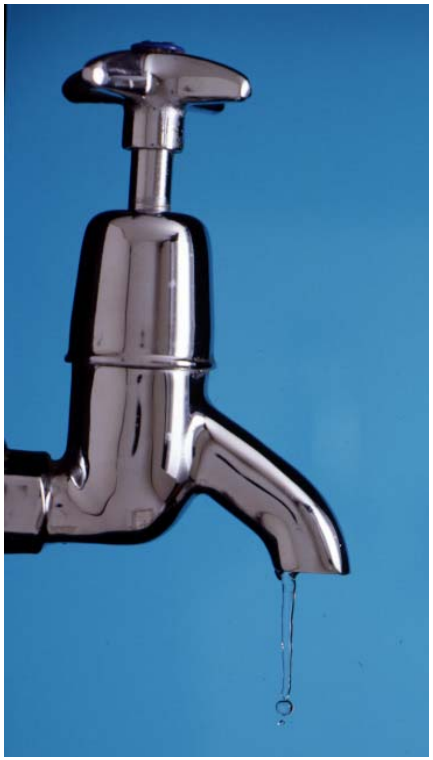
CoreStreet

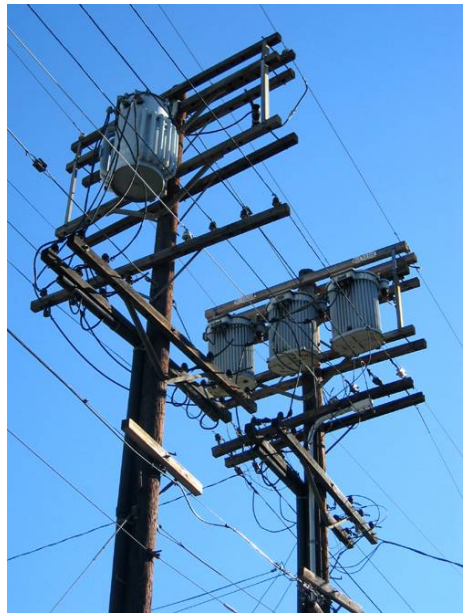
Infrastructure Attributes

- **What are the attributes that the infrastructure requires to fulfill these requirements?**
- **Are there any models in existence that we can use as templates?**
- **Consider identity validation like any societal infrastructure**

CoreStreet

Societal Infrastructure





CoreStreet

Comparing Attributes of Water and Identity Validation

Water

Identity

CoreStreet

Comparing Attributes of Water and Identity Validation

Water

Turn on the tap

Identity

Sub-second response

CoreStreet

Comparing Attributes of Water and Identity Validation

Water

Turn on the tap

Normally able to cope with demand

Identity

Sub-second response

Scalable – used as part of any day's activities

CoreStreet

Comparing Attributes of Water and Identity Validation

Water

Turn on the tap

Normally able to cope with demand

Water available anywhere needed

Identity

Sub-second response

Scalable – used as part of any day's activities

Validation wherever there is a relying party

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	**Highly Available**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	**Accessibility as a right**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	**Resilient – Critical Infrastructure**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	Resilient – Critical Infrastructure
Anonymity of use	**Privacy of user**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	Resilient – Critical Infrastructure
Anonymity of use	Privacy of user
Safe - Just don't mix with electricity……	**Security of use**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	Resilient – Critical Infrastructure
Anonymity of use	Privacy of user
Safe - Just don't mix with electricity……	Security of use
Tap / bottle / distilled	**Quality matched to application/activity**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	Resilient – Critical Infrastructure
Anonymity of use	Privacy of user
Safe - Just don't mix with electricity……	Security of use
Tap / bottle / distilled	Quality matched to application/activity
Water (of varying quality) is global	**Interoperability**

CoreStreet

Comparing Attributes of Water and Identity Validation

Water	Identity
Turn on the tap	Sub-second response
Normally able to cope with demand	Scalable – used as part of any day's activities
Water available anywhere needed	Validation wherever there is a relying party
Interruptions rare	Highly Available
Every household has access to water	Accessibility as a right
Reservoir distribution	Resilient – Critical Infrastructure
Anonymity of use	Privacy of user
Safe - Just don't mix with electricity……	Security of use
Tap / bottle / distilled	Quality matched to application/activity
Water (of varying quality) is global	Interoperability
National or privately operated	**National or Trusted 3rd Parties**

CoreStreet

Advantages of Good Infrastructure

Good infrastructure is resilient !

CoreStreet

Identity Services Infrastructure

A Comprehensive Approach: Identity Services Infrastructure

- **Identity Services Infrastructure (ISI)**
  - A survivable end-to-end system that enables identity-based applications to function in a secure, scalable and reliable manner
  - ISI provides a resilient and comprehensive way to address:
    - Handling millions of individuals (and devices)
    - Multiple authorizations per individual – both on and off card
    - Enhanced security features
    - Future expansion needs
    - High availability/survivability

CoreStreet

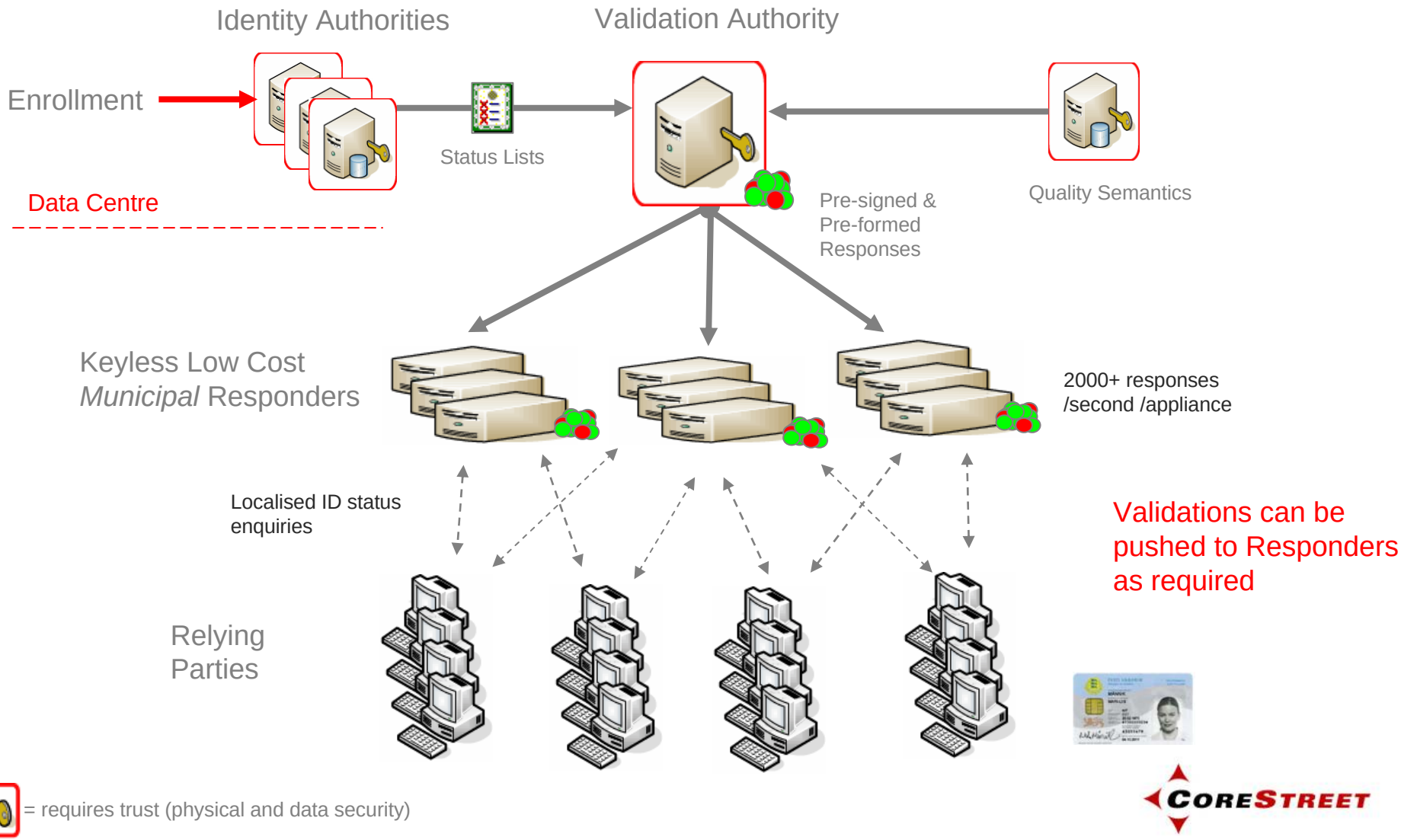
Identity Services Infrastructure Unique Design Principle

Separate the **security sensitive data** and other **trusted operations** from the **delivery process** of providing credential status to relying party applications**.**

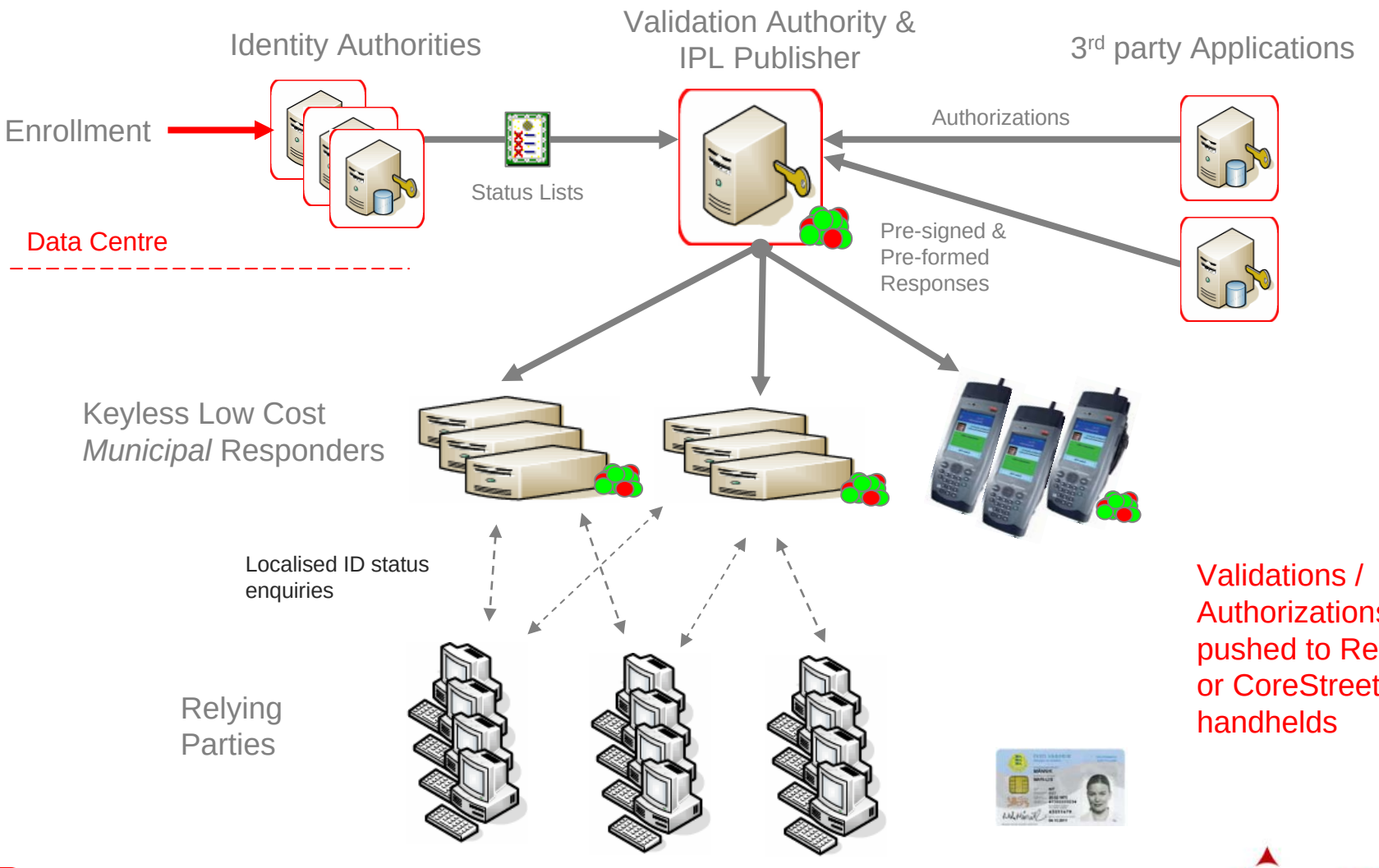
To allow you to start delivering identity services as a utility

CoreStreet

CoreStreet ISI Distributed Validation Principle



CoreStreet ISI Distributed Validation/Authorization Principle

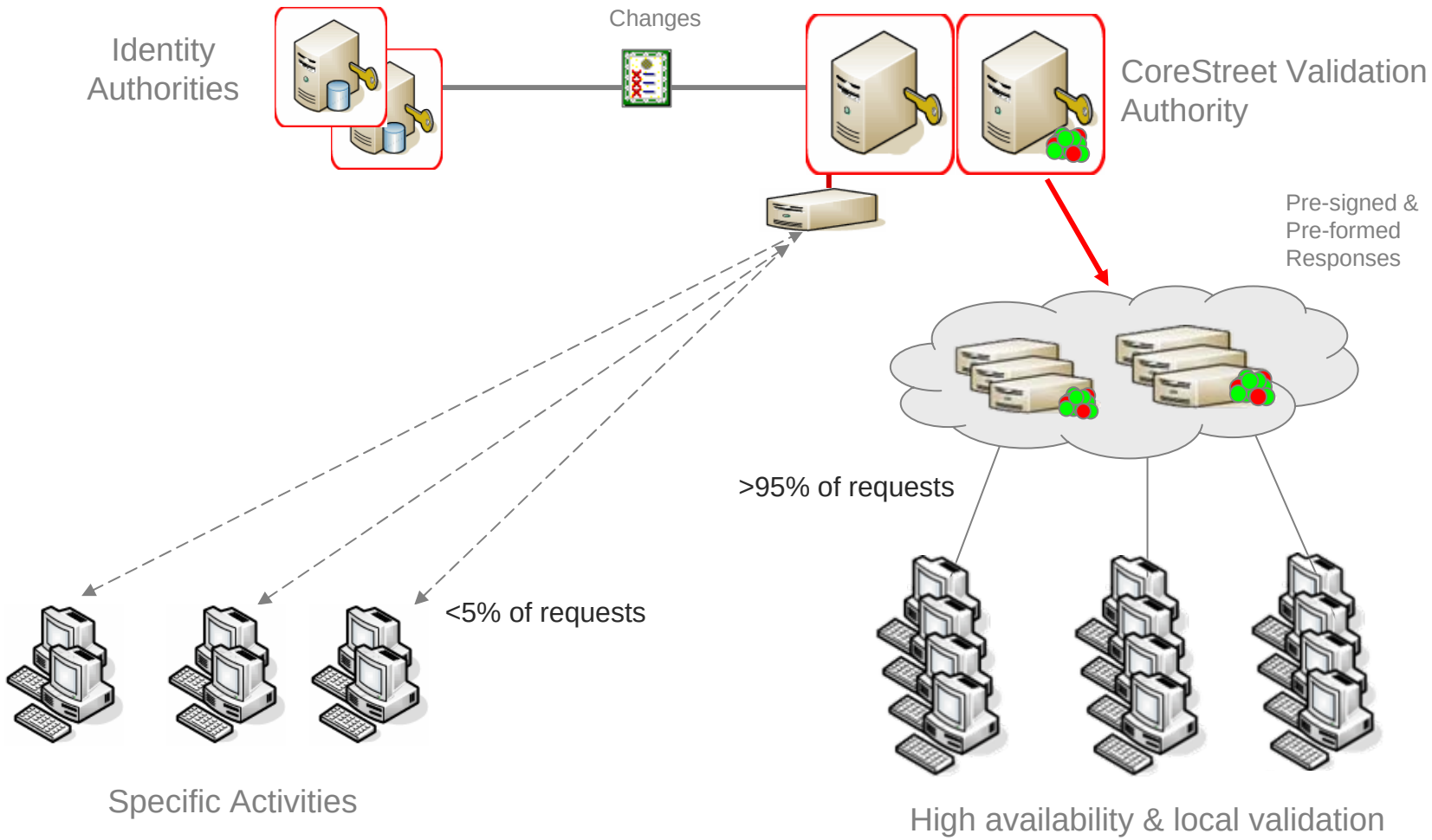


Validations / Authorizations can be pushed to Responders or CoreStreet PIVMAN handhelds

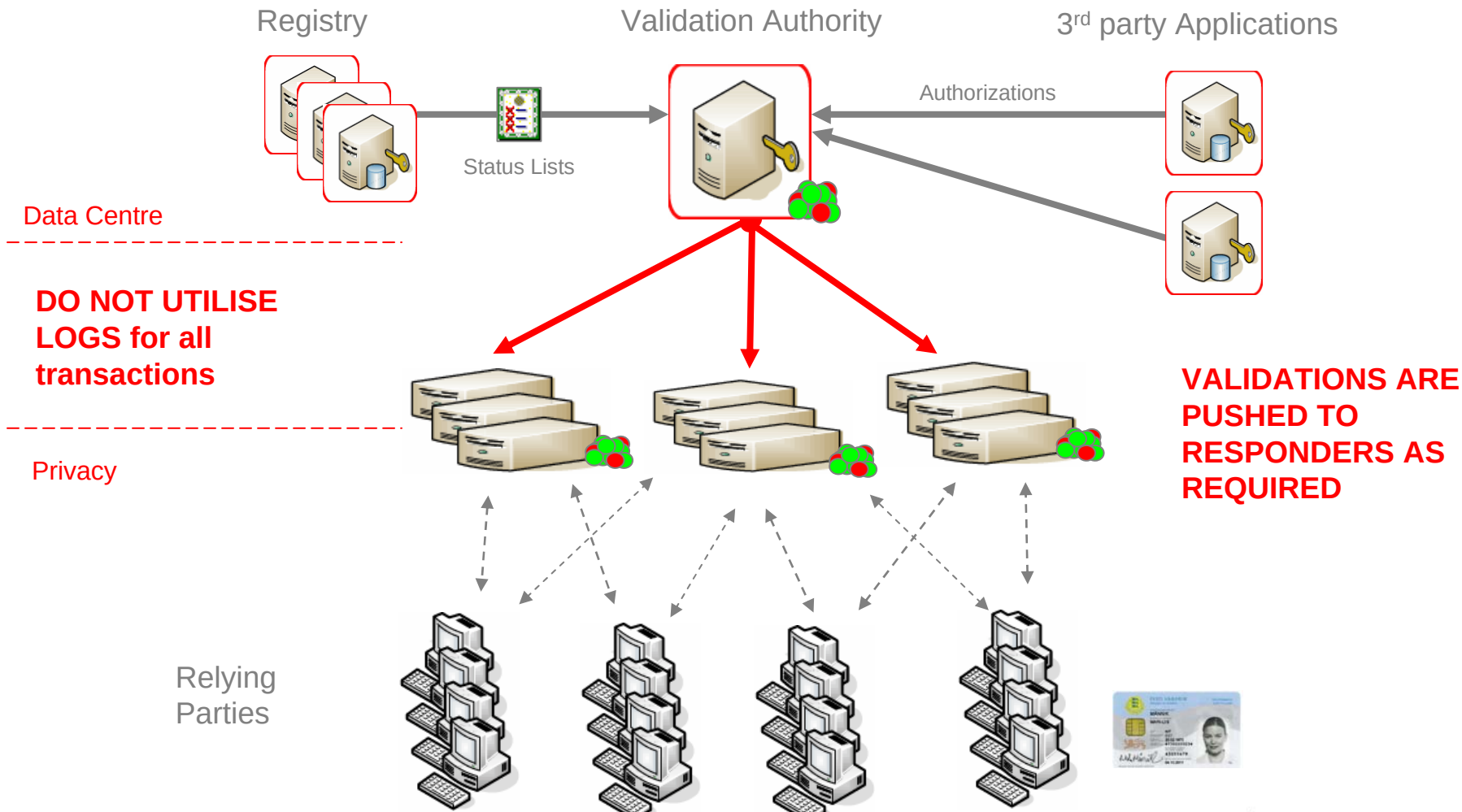
= requires trust (physical and data security)

CoreStreet

CoreStreet ISI Operations Reflecting Appropriate Levels of Validation



Reducing ‘Data Storms’ in CoreStreet ISI



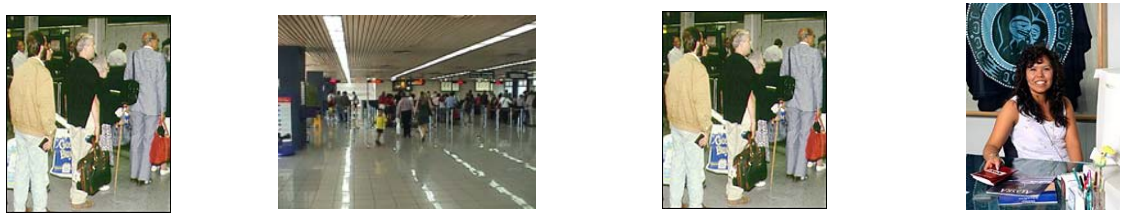
Resilient National ID Cards

Government maintains centralised control of identities whilst providing the essential resilience and fast response to the users

Central Government Validation Authority

Distributed Regional Responders

Relying Agencies and validation activities



Fast and secure validation of ID cards using locally located responders

Alternate Delivery Mechanisms

Mobile/Marine

burst

mobile

disconnected

Disconnected

Connected / web

broadcast

PIVMAN

Government Offices

Global / Remote

Identity Services Infrastructure Components

CoreStreet ISI - Certificate Validation Infrastructure

- Massively scalable **validation technology for use with credential based identity management systems accessed via desktop computers or applications**

Responder 2400

  - Hardware & Software Infrastructure
  - Ultra secure and reliable federation of multiple CA status sources without adverse security impact
  - Fast consistent responses
  - Tamperproof status delivered from locally-based low-cost responders

  - Standards based validation protocols (OCSP, SCVP) and IPL
  - Windows based computers or Windows/Unix/Linux application servers
  - Out-of-the-box connections to Certificate Authorities and other data stores

CoreStreet

CoreStreet Autonomous Validation PIVMAN

- **Delivers the validation status of a large user population to an autonomous and disconnected devices using IPL**
- **Highly secure and tamperproof**
  - Very low bandwidth required for synchronising data
  - Low storage requirement:
  - approx 250K per million validation records
  - Provides positive validation

Example: PIVMAN Handheld

CORESTREET

CoreStreet ISI – Feature Summary

- Resilience
  - Validation during non continuous communications
  - Improved Service Levels
- Usability
  - Low latency local responders: fast responses
  - High availability: better than 2000 responses/sec/responder;
- Flexibility
  - Responders can be set up in minutes whenever with no security impact.
  - Disconnected and handheld capability
  - Can accommodate legacy validation requirements
- Scalability
  - Can scale cost-effectively to hundreds of millions of credentials
  - Authorizations are incorporated in the responses
- Security
  - Air gap capability Credential Authority.
  - Responders are keyless and DO NOT need to be vaulted

CoreStreet

ISI Deployment Case Study

Case Study: U.S. Government Common Access Card

- **A US agency was looking for a validation solution to manage all 4.5 million employees. (As a result of the recent Presidential mandate HSPD12, the total number of federal users will grow to 40+ million)**
  - Before ISI
    - Centralised vulnerable architecture
    - Systems too slow to function
    - Security concerns around private key protection
    - Cost of scaling meant implementations were kept small
  - Post ISI implementation
    - Inbuilt resilience
    - Response times dropped to less than one second - globally
    - The system can scale to meet all future needs, including government-wide implementation without cost concerns
    - Security was significantly increased

CoreStreet

Example Partners & Certification

•CoreStreet Validation Authority is National Information Assurance Program (NIAP) Common Criteria EAL 3+ certified

CoreStreet

Criteria for Success

Success Criteria for National ID / eID

“Thank you for my ID Card !”

CoreStreet

Questions?

Thank You

Jon Shamah
CoreStreet EMEA
jshamah@corestreet.com

PHONE: +44 (0) 7813 111290
FAX: +44 (0) 20 8357 6460