



CREDENTIALICA

# Non-Intrusive Identity Management

Dr. Stefan Brands

McGill School of Computer Science & Credentica

April 12, 2004

Presented to: 3<sup>rd</sup> Annual PKI R&D Workshop, Gaithersburg

# Personal credentials (1)

credentica.com



- **Adjunct professor at McGill Univ. (Comp. Sc.)**
  - Co-supervising master's and PhD students
  - Member of SSHRC privacy project "On The Identity Trail"
- **Professional cryptographer since 1992**
  - Secure electronic authentication
  - Cross-domain access control & identity management
  - Privacy-enhancing/preserving technologies
  - Electronic payments
- **Member of External Advisory Board of Privacy Commissioner of Canada**
- **Member of CSIS Authentication Working Group**
  - Co-chaired by Lawrence Lessig and Craig Mundie

# Personal credentials (2)

credentica.com



- **Author of MIT Press book “Rethinking Public Key Infrastructures; Building in privacy”**
  - Updated version of dissertation (1992-1996 ... 1999)
  - Thesis advisor: prof. Adi Shamir of Weizmann Inst. (**RSA**)
  - Foreword: prof. Ronald L. Rivest of MIT (**RSA**)
    - *“an important landmark in the evolution of privacy-enhancing technology”*
- **Lots of “real-world” experience with privacy & secure authentication technologies:**
  - Consultancy
  - Principal protocol designer of EU-piloted e-purse system
  - Senior cryptographer at privacy-technology companies
    - DigiCash (1996-1998)
    - Zero-Knowledge Systems (2000-2001)
  - Currently with Credentica (2002-...) Funded by Nokia

# Content

credentica.com



- **Part I**
  - PKI & digital identity management
- **Part II**
  - Digital Credentials
- **Appendix A**
  - PKI & cross-domain access control (details)



# PKI – historical perspective

credentica.com



- **1976: Invention of public-key cryptography:**
  - Setting: Message encryption over open network
  - Sender encrypts message with **public key** of recipient
  - To prevent man-in-the-middle attack: rely on on-line database specifying name–public key bindings
- **1978: Kohnfelder (bachelor’s thesis):**
  - Database: bottleneck & vulnerable to attacks
  - **Identity certificates** proposed to address this problem
- **1990’s: X.509 identity certificates provide:**
  - **Confidentiality** of data in transit (through encryption)
  - **User authentication** (ensures messages are encrypted under right public key & prevents man-in-the-middle attack)
  - **Data integrity** (prevent tampering with data in transit)
  - **Non-repudiation** (proof of sender’s identity)

# PKI – what is it good for?

credentica.com



- **Message encryption**
  - SSL encryption, secure e-mail
- **Message signing**
  - Document signing, code signing, notarizing, ...
- **“Inescapable” identity**
  - *“Your digital passport to the information highway”*
  - SSL authentication, ...
- **Single-domain access control**
  - Approach (by stretching PKI ...):
    - Access requestor must show identity certificate
    - Certificate = authenticated pointer to back-end database entries
    - Access provider retrieves data for **authorization** decision
  - VPN access, organizational SSO, ...

# PKI – what is it NOT good for?

credentica.com



- **Cross-organizational access control**
  - Problems certificates were supposed to address are back (with a vengeance!)
    - Bottleneck of real-time database consulting
    - **Online** database vulnerabilities
  - Need additional security safeguards
    - Cloning of access rights
    - Lending of access rights
  - Privacy problems
    - Like credit card infrastructure on steroids
    - For organizations towards central parties
    - For individuals towards organizations & central parties
- **Cross-organizational identity management**
  - Access control + information sharing/linking/reuse

# Digital identity management (1)

credentica.com



- **Network identity**
  - Collection of information relating to an individual
  - Created and managed as single unit in a network
  - Stored in electronic form
- **Situation today:**
  - Individuals have many fragmented network identities
  - Aggregating network identities is increasingly easy
  - But: which network identities pertain to **same** individual?
    - If linkage is wrong, aggregate has less value (**data pollution**)
- **Causes of pollution**
  - Unintentional (different name spellings, ...)
  - Intentional (avoidance, theft, lending, copying, forgery, insider help, ...)

# Digital identity management (2)

credentica.com



- **To derive value: network identities must be accompanied by unique cross-domain identifiers**
- **Simple approach:**
  - Request / capture identifier when collecting data
    - Employee ID, static IP address, health insurance number, SSN, credit card number, passport ID, biometric, **X.509 certificate**, ...
  - Aggregate on basis of cross-domain identifier
    - Physical aggregation or logical/virtual aggregation
- **Need to consider different settings**
  - Intra-organizational: Enterprise identity management, ...
  - Extended organizational: extended enterprise (SCM), ...
  - Cross-organizational: E-health, E-government, Critical Information Infrastructures, E-commerce, ...

# Where does this approach work fine?

credentica.com



- **Single-domain intra-organizational**
  - Employees have low/no privacy expectations/rights
  - Trust dynamics very simple
  - No scalability issues
  - Can use traditional security tools (“silo protection”)
    - Door guards, intrusion detection, firewalls, anti-virus, ...
- **Multi-domain intra-organizational (branches, ...)**
  - Trust dynamics minimally complicated
  - Low privacy expectations
  - Possibly some scalability issues
  - Traditional security tools still work
- **Large organization with satellite organizations**
  - Authentication relation already unbalanced

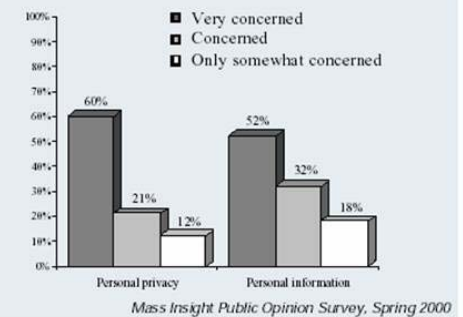
# Where does it break down?

credentica.com



- **“Balanced” business-to-business (B2B)**
  - Collaborative enterprise applications
- **Government-to-business (G2B)**
- **Business-to-consumer (B2C)**
- **Government-to-citizen (G2C)**
  - Implications for stability of democracy
- **Consumer-to-consumer applications**
  - Online gaming, instant messaging, ...
- **Peer-to-peer transactions**
- ...

Concern over “personal privacy” and “keeping personal information private.”



# Privacy & personal information

credentica.com



- **Privacy:** *“The right of individuals, groups, and organizations to determine for themselves when, how, and to what extent information about them is communicated to others.”*
- **Different manifestations for:**
  - Individuals (ROI hard to quantify)
  - Companies (competitive intelligence, liability)
  - Critical Information Infrastructures (monitoring)
- **Personal information:** *“information about a data subject whose identity can reasonably be ascertained from the information”*
- **Network identity = personal information !**
  - Unless **NO PARTY** other than the data subject can determine who is behind a network identity
- **Data protection legislation: organizations must protect personal information**

# Fair Information Principles (FIPs)

credentica.com

## OECD FIPs:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security safeguards (incl. confidentiality)
6. Openness
7. Individual Participation
8. Accountability

Technology can address security needs **without** addressing privacy, but this may **introduce grave new security** concerns!

Security safeguards deal mainly with **unauthorized outsiders**, but most privacy threats come from **insiders**

# PKI “quick fixes” that do not work (1)

credentica.com



- **Identity certificates specifying a “pseudonym” or a “role” instead of a real name:**
  - Does not address privacy problems (tracing on basis of **public keys/CA signatures** in certificates!)
  - Weakens security (accountability, fraud containment, ...)
  - All other problems remain
- **X.509 attribute certificates**
  - Addresses **only** availability problem
    - Attribute certificates must be linked to (and sent along with) base identity certificate to **prevent pooling of privileges**
  - All other problems **worsen:**
    - **More** privacy-invasive (attributes within certificate known to CA & disclosed when showing certificate)
    - No security mechanisms to prevent discarding, updating-prevention, lending, and cloning (easier when in database!)
    - Must manage and revoke an abundance of certificates

# PKI “quick fixes” that do not work (2)

credentica.com



- **Different CA & certificate per domain:**
  - False sense of privacy:
    - Like using SSNs and credit card numbers for all actions
    - Privacy worse due to fully electronic nature
  - Creates “islands” that cannot communicate
    - Greatly reduces functionality for all participants
      - Inform sharing no longer possible
      - SSO goes out the window
    - Only way to link is through bridging CAs
      - This violates what we were trying to achieve
  - Inefficient for client
    - Multiple certificate management
    - Smartcard can hardly handle a single certificate
  - Security limitations
    - no cross-domain revocation

# What about federated identity management?

credentica.com



- **Centralize authentication power from different domains into a central domain**
  - Maps cross-domain context back to single-domain context
  - Apply single-domain authentication techniques
    - Password-only, Kerberos, PKI, biometrics, ...
- **Leave authorization decisions at original domains**
- **Liberty Alliance:**
  - Circle of trust: “SPs” using a central “IdP”
  - Counter-movement to Microsoft’s Passport
    - IdP (Microsoft) collected user data, not SPs themselves
  - Allows many circles of trust
  - Allows any single-domain authentication technique
  - User can be known under different pseudonym at each SP

# What is it good for?

credentica.com



- **IdP is like a Visa in its “circle of merchants”**
  - Can track, trace, and link all interactions in real time
  - Can impersonate users across circle of trust
  - Can deny access to users across entire circle of trust
  - Appealing target for hackers, insiders, DOS attacks
- **OK if legacy system mirrors this power relation**
  - Intra-organizational identity management
    - Multiple branches
    - Affiliates
  - “Unbalanced” B2B
    - IdP is powerful institution with pre-existing powers over SPs
- **No good in general cross-organizational contexts**
  - User concerns
  - SP concerns

# Needed: new authentication primitives!

credentica.com



- **Traditional authentication primitives meet only limited requirements:**
  - Security against unauthorized outsiders
  - Efficiency
  - Scalability
- **Cross-domain access brings NEW requirements**
  - Complicated trust dynamics
  - Vulnerabilities due to (real-time) reliance on central parties
    - Denial of service, hackers, insiders
  - Security against dishonest insiders
  - Perimeter security techniques of little use
    - All security must be tied to the information itself
  - Privacy: Control over who can learn what information



# Digital Credentials

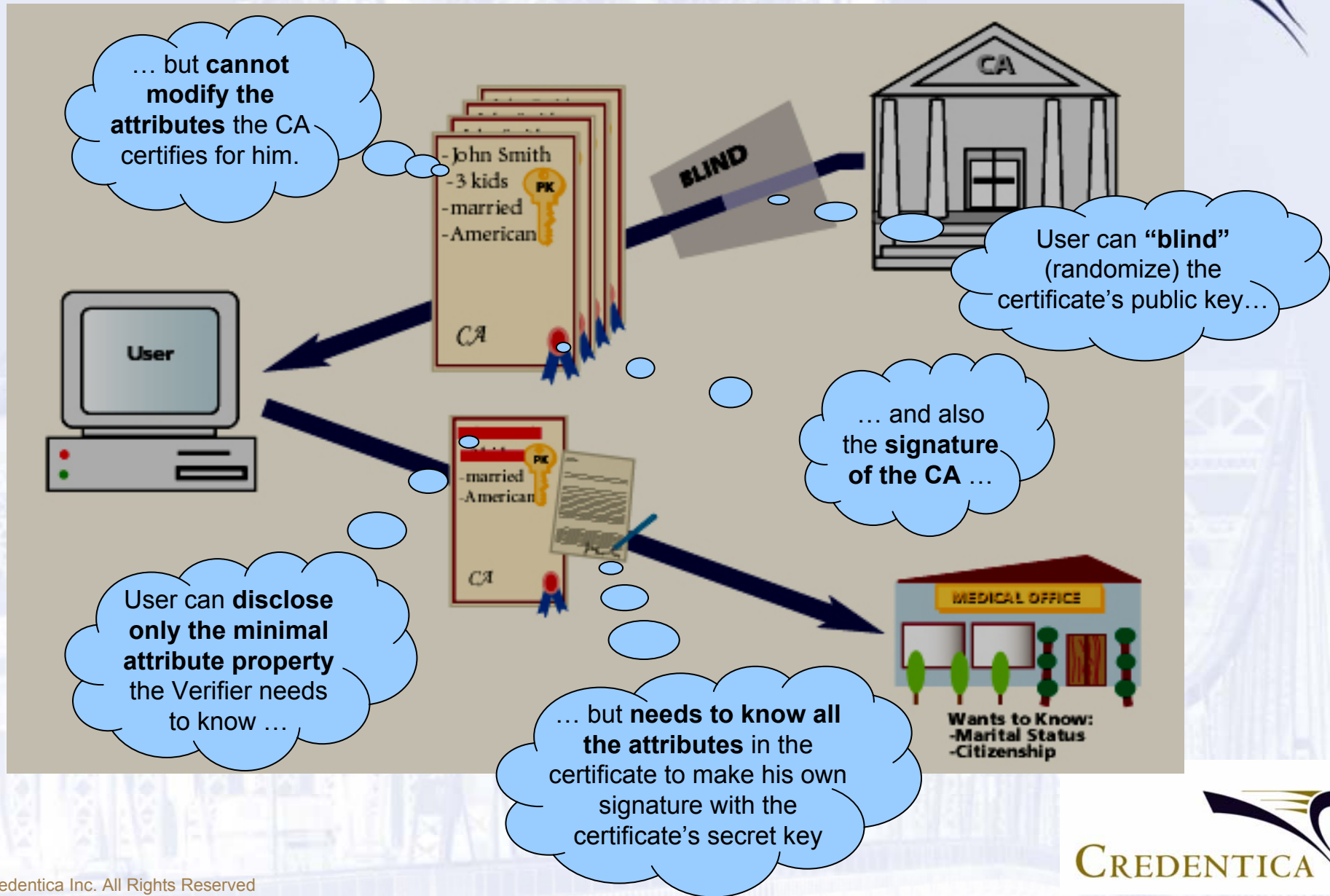
credentica.com



- **Based on 20 years of academic research**
  - Dozens of reputable academics, starting with groundbreaking visionary work by Chaum
- **All the strengths of digital certificates, but much more powerful**
  - One certificate can contain many arbitrary attributes
  - Separate privacy & security sliders
  - **Unlinkable** certificate issuing and showing
  - User can **selectively disclose** attribute properties
  - Identification, anonymity, pseudonymity, “in between”
  - Program can **selectively hide** disclosed attributes
  - Unique security features
  - Efficient smartcard implementation

# Digital Credentials in action

credentica.com



# Properties of Digital Credentials (1)

credentica.com



- **Fully adaptable levels of privacy:**
  - Anonymous, pseudonymous, role-based access, and anything “in-between”
  - Principle of least authority; **selective/minimal disclosure**
  - Reverse authentication: data does **not** meet conditions
  - **Recertification and updating:** present Digital Credential without revealing current attribute values
  - Dossier-resistance: leave no or partial non-repudiable transaction evidence to verifier
  - Credential verifier can **selectively hide** data before passing on digital evidence 3<sup>rd</sup> party
  - Credential Authorities can be prevented from learning the attributes that they certify
  - Smartcard cannot leak sensitive data to outside world

# Properties of Digital Credentials (2)

credentica.com



- **Security protections:**
  - No **pooling** of privileges (multiple Digital Credentials can be shown to contain same identifier without disclosing it)
  - **Lending** protection: Embed client-confidential data into Digital Credential (legitimate owner need never disclose it)
  - **Discarding** protection: Lump negative data in base Digital Credential (e.g., drunk driving mark into driver's license)
  - **Limited-show** credentials: Embedded identifier (or value) exposed if and only if Credential shown too many times
  - Audit capability:
    - Digital audit trails & receipts facilitate dispute resolution
    - Non-identified audit trail cannot be disavowed by originator
    - Self-signed fraud confessions for lending and reuse

# Properties of Digital Credentials (3)

credentica.com



- **Smartcard Implementations:**

- Manage billions of Credentials using 8-bit smart-card chip (off-load storage and computational burden to user device)
- Application provider can arbitrarily minimize level of trust placed in smartcard (through application software)
- Secure multi-application smartcards:
  - Different application providers can share same secret key
  - Digital Credentials have uncorrelated secret keys (unknown even to card supplier) and can be revoked separately
  - Different applications using same smartcard are fire-walled through user software (not card software!)
  - Leakage of a card's key does not allow fraud beyond the security functionality the card was supposed to add

# Properties of Digital Credentials (4)

credentica.com



- **Managed services:**
  - Credential Authorities certify sensitive information without being able to learn the data
  - Revocation Authorities can validate certificates without being able to identify the clients of organizations
  - Role of tamper-resistant smartcard can be outsourced
- **Peer-to-peer support:**
  - Individuals can store and manage their own credentials
  - Unauthorized users cannot modify, discard, lend, pool, or prevent the updating of information they hold
  - Distribute all back-end database entries to data subjects
  - Multi-purpose and multi-application certificates

# Issuing protocol (example)

USER

CERTIFICATE ISSUER

$$h := g_1^{x_1} g_2^{x_2} g_3^{x_3}$$

$$w_0 \in_{\mathcal{R}} \mathbb{Z}_q$$

$$a_0 := g_0^{w_0}$$

$$\xleftarrow{a_0}$$

$$\alpha_1 \in_{\mathcal{R}} \mathbb{Z}_q^*$$

$$\alpha_2, \alpha_3, w_1, w_2, w_3 \in_{\mathcal{R}} \mathbb{Z}_q$$

$$h' := (hh_0)^{\alpha_1}$$

$$a := (h')^{-w_1} g_1^{w_2} g_3^{w_3}$$

$$c'_0 := \mathcal{H}(h', a, a_0 g_0^{\alpha_2} (hh_0)^{\alpha_3})$$

$$c_0 := c'_0 - \alpha_2 \pmod q$$

$$\xrightarrow{c_0}$$

$$r_0 := (w_0 - c_0)(x_0 + \sum_{i=1}^3 x_i y_i)^{-1} \pmod q$$

$$\xleftarrow{r_0}$$

$$g_0^{c_0} (hh_0)^{r_0} \stackrel{?}{=} a_0$$

$$r'_0 := (r_0 + \alpha_3) \alpha_1^{-1} \pmod q$$

# Showing protocol (example)

credentica.com



USER

$$c := \mathcal{H}(h', a, \text{spec})$$

$$r_1 := -c\alpha_1^{-1} + w_1 \text{ mod } q$$

$$r_2 := -cx_1 + w_2 \text{ mod } q$$

$$r_3 := -cx_3 + w_3 \text{ mod } q$$

VERIFIER

$$(h', a), (c'_0, r'_0), x_2, (r_1, r_2, r_3)$$

$$c'_0 \stackrel{?}{=} \mathcal{H}(h', a, g_0^{c'_0} (h')^{r'_0})$$

$$c := \mathcal{H}(h', a, \text{spec})$$

$$(h')^{r_1} a \stackrel{?}{=} g_1^{r_2} g_2^{-x_2 c} g_3^{r_3} h_0^{-c}$$

# Details: “Rethinking PKI; building in privacy”

credentica.com

***“an important landmark”***

Dr. Ronald L. Rivest (Webster Professor of Electrical Engineering and Computer Science at MIT), August 2000

***“minimizing the risks of all the interested actors”***

Electronic Privacy Information Center & Privacy International, 2001

***“a superior alternative to conventional approaches to PKI”***

Dr. Roger Clarke (consultant in the management of information and information technology), 2001

***“security without sacrificing privacy”***

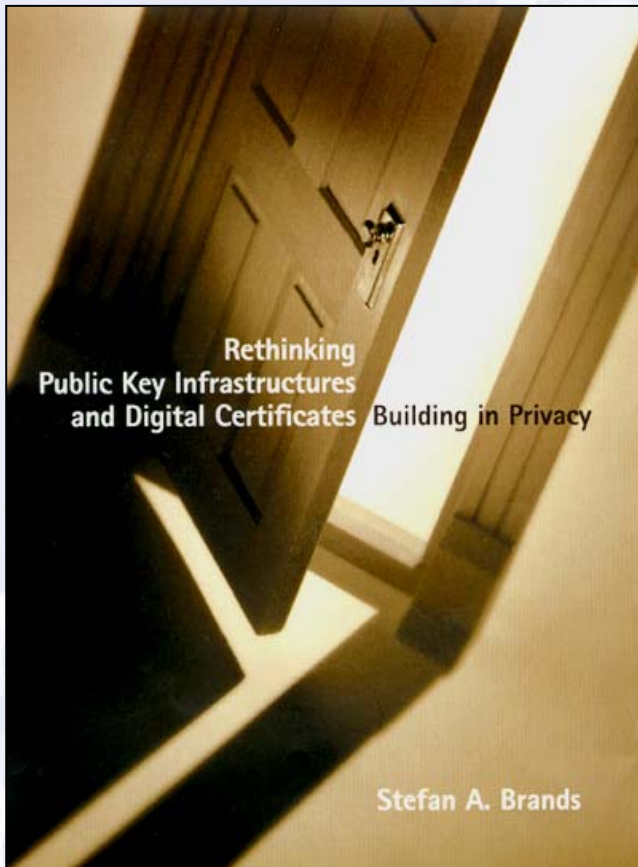
Dr. Hal Abelson (Professor at the Artificial Intelligence Laboratory, MIT), August 2000

***“the state of the art”***

Dr. A. Michael Froomkin  
(Professor of Law, University of Miami), August 2000

***“digital certificates without giving so much power to the system owner”***

Former Chief Privacy Counselor to the Clinton Administration, Dr. Peter Swire, April 2001





# Appendix A

## PKI & cross-domain access control (details)

# PKI & access control: problems (1)

credentica.com



- **Unscalable beyond pre-established domains:**
  - Access provider relies on the availability, correctness, and timeliness of authorization data
- **Poor security:**
  - Access right cloning and lending: no cryptographic protection
  - Misuse of online databases by hackers and insiders
  - Vulnerable to denial-of-service attacks:
    - Strong reliance on real-time availability of online databases
    - Online certificate status validation
  - Increases risk of identity theft:
    - Inescapable system-wide identification
    - Strong reliance on central databases

# PKI & access control: problems (2)

credentica.com



- **Not suitable for use with smartcards:**
  - Cannot use low-cost smartcards:
    - Storage problem
    - Need crypto co-processor for exponentiations
    - Elliptic-Curve cryptography is only partial solution
  - Application provider **must place very strong trust** in parties involved in smartcard manufacturing, masking, initialization, application loading, and personalization.  
Attacks:
    - Overt or covert leakage of secrets and other confidential data
    - Uniqueness, randomness, and secrecy of secret keys??
    - Fake-terminal attacks
    - Selective “failure” attacks based on dynamic inputs
  - Problems worsen for multi-application smartcards

# PKI & access control: problems (3)

credentica.com



- **Managed services are intrusive:**
  - Online Certificate Status Providers able to learn competitive/sensitive data in real time:
    - Identities of access requestors (and access providers)
    - Peak hours
    - Typically: nature of the transaction
    - Possibly: transaction details
  - Certificate Authorities must know the identity and any other attributes that go into the certificates they issue
  - Online Certificate Status Providers & Certificate Authorities & on-line database maintainers can **disrupt operations** on the basis of transaction-specific knowledge **in real time**

# PKI & access control: problems (4)

credentica.com



- **Privacy-invasive (inescapable systemic identification rooted into infrastructure):**
  - Public keys = strongly authenticated “super-SSNs”:
    - **Globally unique** identification numbers
    - **Inescapably travel along** with each and every action taken
    - Obtained by access provider **& third parties** (providers of authorization databases & online certificate status verifiers)
  - Always leave behind **undeniable digital evidence** of the requestor’s identity (due to digital signing of nonces)
  - Problems with data protection legislation, unbridled use of PKI may be unconstitutional
  - Access providers & 3<sup>rd</sup> parties **cannot prevent** receiving identifiable data