



CREDENTICA

Identity: Setting the Larger Context, Achieving the Right Outcomes

Dr. Stefan Brands
November 3, 2006

7th Annual Privacy and Security Workshop &
15th CACR Information Security Workshop

“Achieving the right outcomes” – of what?

credentica.com



- **Focus of this presentation:**
 - (Large-scale) identity systems
- **To achieve “the right outcomes” one must meet:**
 - Functional requirements (SSO, PIM, data sharing, ...)
 - Security requirements
 - Interoperability
 - Flexible roadmap (evolution)
 - Privacy (often not an explicit requirement ...)
- **Key ingredients to success:**
 - Identity policy (relating to privacy)
 - Data protection legislation / FIPs
- **Policy and law must be “technology-neutral”**
 - But NOT technology-unaware!!

Identity management basics

credentica.com



- **Single-domain identity management (“silo”)**
 - Quite well represented by FIPs
 - Quite well understood by policy makers
 - (However: automation continues to increase risks)
- **Cross-domain identity management**
 - Breaking out of the “identity silos” (electronically!)
 - To enable (unanticipated) “secondary uses” ...
 - Typical data “shared” across domains (a la SAML):
 - Authentication statements, attribute statements, authorization decision statements
- **Policy and law have NOT caught up!**
 - Must be concerned with CROSS-DOMAIN data sharing
 - Requires NEW policies and FIPs

Technologies for single-domain identity

credentica.com



- **Data repositories**
- **Provisioning of identity data WITHIN silos**
 - Tools for managing “user accounts” (creation, deletion, I/O)
- **Access management**
 - Authentication and authorization to protect resources
 - Policy engines, policy expression languages
- **Auditing and compliance**
 - Track how data is created, modified and used
- **User administration**
 - Account access reset, delegation, approval workflow, ...
- **Data security**
 - Data authenticity, integrity, encryption (in transit and at rest)

Technologies for cross-domain identity

credentica.com



- **All single-domain technologies (augmented)**
- **“Discovery” services**
- **Simplified/Single Sign-On (SSO)**
- **Cross-domain data sharing “glue”**
- **Technologies for “linking up” accounts!**
 - “Back-end” statistical linking tools to match accounts
 - “Federation” (a la SAML / ID-FF, ID-WSF)
 - Electronic approach whereby user establishes account linkages
 - Identity data flows from source to destination (no user “control”)
 - User-centric identity management
 - Identity data flows through user (data subject) to relying party
 - User can be given actual control over his/her personal information
 - Boon to privacy or its worst nightmare?

User-centric identity: “heavyweight” efforts

credentica.com



- **Microsoft CardSpace (formerly InfoCard)**
 - “Windows” UI component and related services for managing identity “cards”
 - User can select cards (“identity selector”)
 - Improved protection against local viruses
 - Self-issued and managed identity cards
 - Managed identity cards issued by identity providers
 - Any technology that supports WS-* protocols can integrate
- **Liberty Alliance iClient/TMa**
 - Expanding Liberty Alliance ID-WSF protocols to support intelligent clients for storing and managing credentials
 - ID-FF supports browser redirects only (“zero-footprint” browser)
 - Driven by Intel and NTT

User-centric identity: “lightweight” efforts

credentica.com

- **Higgins project (IBM, Novell, small players):**
 - APIs for integrating identity data across multiple systems
 - SAML, CardSpace, ...
- **OSIS (open source effort)**
 - Building “identity selectors” compatible with CardSpace
- **OpenID (subsuming DIX and LID)**
 - **Lightweight** Web SSO for URL-based authentication
 - Aimed at blogging community (not security-focused)
- **Bandit**
 - Novell-sponsored attempt at common identity framework
- **Heraldry Identity Project:**
 - Apache Software Foundation effort using Yadis/ OpenID

“Laws” of identity (Microsoft & IPC of Ontario)

credentica.com



- **User Control and Consent**
 - User can store own identity data and control its release
- **Minimal Disclosure for a Constrained Use**
 - Limit scope for unauthorized secondary uses
- **Justifiable Parties**
 - A party’s involvement in identity relations must be justifiable
- **Directed Identity**
 - Unidirectional identifiers for users to minimize linkage across sites
- **Pluralism of Operators and Technologies**
- **Human Integration**
- **Consistent Experience across Contexts**

User-centrism: pro-privacy characteristics

credentica.com



- **Can the data subject:**
 - Pick his own IdP to meet the RP's requirements?
 - Like having your pick of credit card issuer ...
 - Consent to or withhold its release
 - On case-by-case basis, informed, non-coerced, ...
 - Hide the identity of the RP from the IdP?
 - Hide the RP's request from the IdP?
 - See the actual identity data?
 - Or is it encrypted for SP ...
 - Selectively disclose attribute data on identity credentials?
 - Locally store and manage **long-lived** identity credentials?
 - Avoid **correlation handles** across IdPs and SPs?
 - Or are data subjects (unknowingly) linking up all of their account relations with each and every disclosure?

User-centrism: boon or nightmare to privacy?

credentica.com

- **Data subject as “choke point” is NOT enough**
- **User-centrism at its worst (for privacy):**
 - User greatly EXTENDS the cross-domain sharing of identity data about him or her
 - Each user-centric data transfer creates a common cross-domain user identifier/handle
 - The user accelerates the “federation” of his account information!
 - Once accounts are federated, user is powerless:
 - Organizations can freely exchange user data without user involvement
 - Identity thieves can freely cross what used to be identity “silos”
- **CardSpace is an ENABLER of PETs, not a PET**
 - Current version does not comply with the “laws” of identity
 - MUST be used in conjunction with PETs

User-centrism without PETs is bad for privacy!

credentica.com

“The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.”

Privacy Protection Study Commission,
Personal Privacy in an information Society,
(July 1977)

Example of pro-active government: Quebec

credentica.com

- **Projects: ClicSÉQUR and L'Espace Citoyenne**
 - *“The government must ... implement institutional mechanisms, and even laws, to promote the use of specific **technologies for protecting personal information and privacy**. ... We recommend that the government look into the possibility of **establishing a legal framework** to ensure that the technologies comply with the imperatives regarding the protection of privacy (**privacy-compliant and privacy-enhancing technologies**).”* -- Minister Gautrin, Quebec E-Government roadmap report, June 2004
 - *“Requirements on the protection of the personal information: ... allowing citizens to only use **pseudonyms** and giving them free choice over their pseudonyms; to limit the possibility of **linking** identity data; to limit the possibility **WITHIN THE GOVERNMENT APPARATUS** of **tracing** the use of identifiers.”* -- RFI on authentication solutions

Proposal for a new Fair Information Principle

credentica.com

- ***“An organization must obtain explicit legal authorization if it wants to obtain a unique identifier from a user that has already been associated with that same user by another organization”***
 - Even better: *“... that can be correlated with any identifier of the same user in another domain”*
- **Notes:**
 - Inspired by SIN/SSN legislation
 - This would encourage organizations to use **independently** generated identifiers to transact with their clients
 - An “identifier” is any information that can be (efficiently) resolved to a unique person/user without requiring that person’s active cooperation

