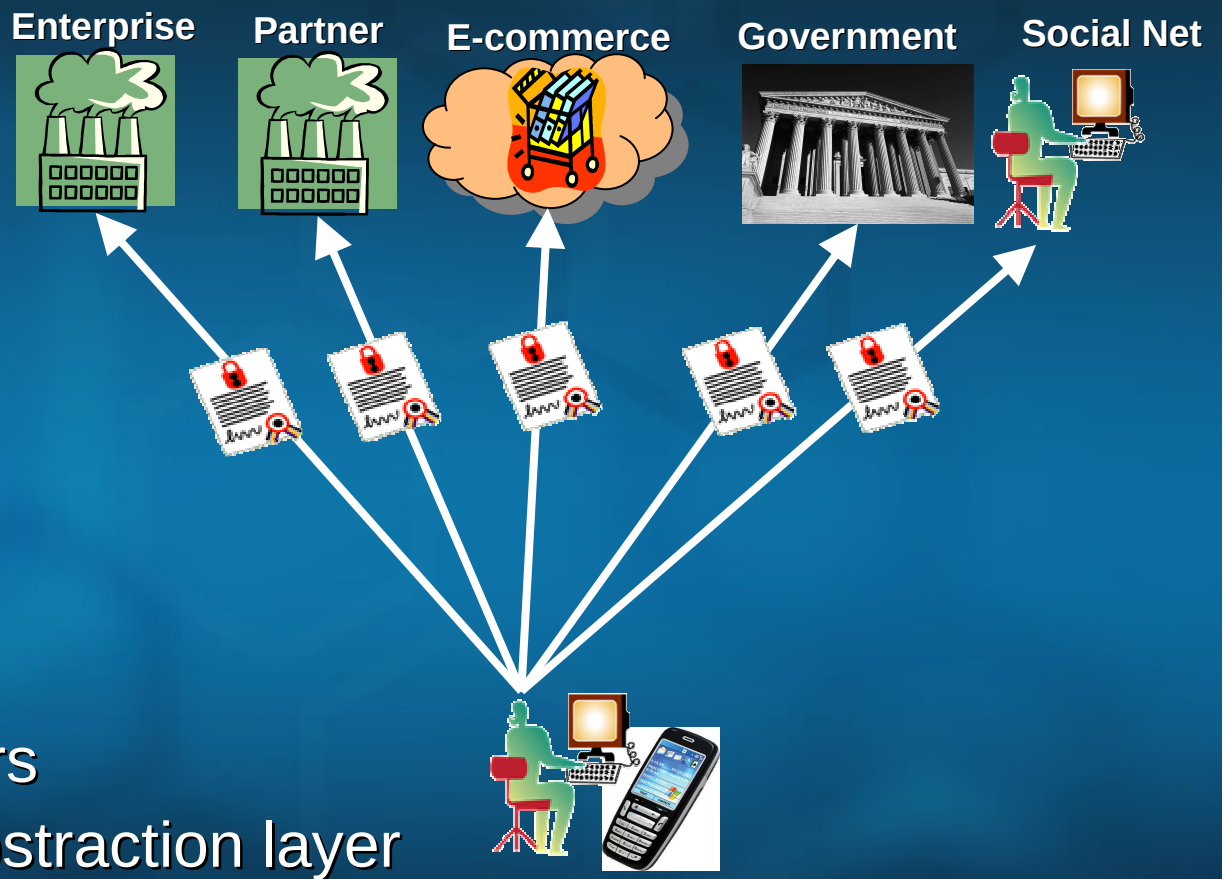
Claims-Based Identity Layer for the “New Internet”

Slava Kavsan,
Partner Architect
Microsoft Corp.

Topics

- Need for the Internet Identity Layer
- Claims-based Identity model
  - Laws of Identity and Identity Metasystem
  - Claims taxonomy
  - Claims transformation model for access
  - Authentication, role of Personal Trusted Devices
  - Federated Identity
  - Identity and Access Management

Seamless, Easy and Trusted Identity



What will it take?

- Redefined perimeters
- Standards-based abstraction layer
- Unified interfaces for use and programming
- Agile cooperating systems – rendezvous of capabilities

Missing Internet Identity Layer

- Identity layer – architectural hole in the Internet
- OSI/X.500 scratched the surface, did not succeed
- Not addressed in the current “short” Internet stack (IPv4, IPv6)
- PKI offers a solid foundation, but serious limitations exist
- Result: identity ad hoc quasi-layer in applications and protocols

What is a Digital Identity?

- Set of *claims* made about a subject
- Many “sets” for many uses
- Required for transactions in real world and online
- Model on which all modern access technology is based

“The Laws of Identity”

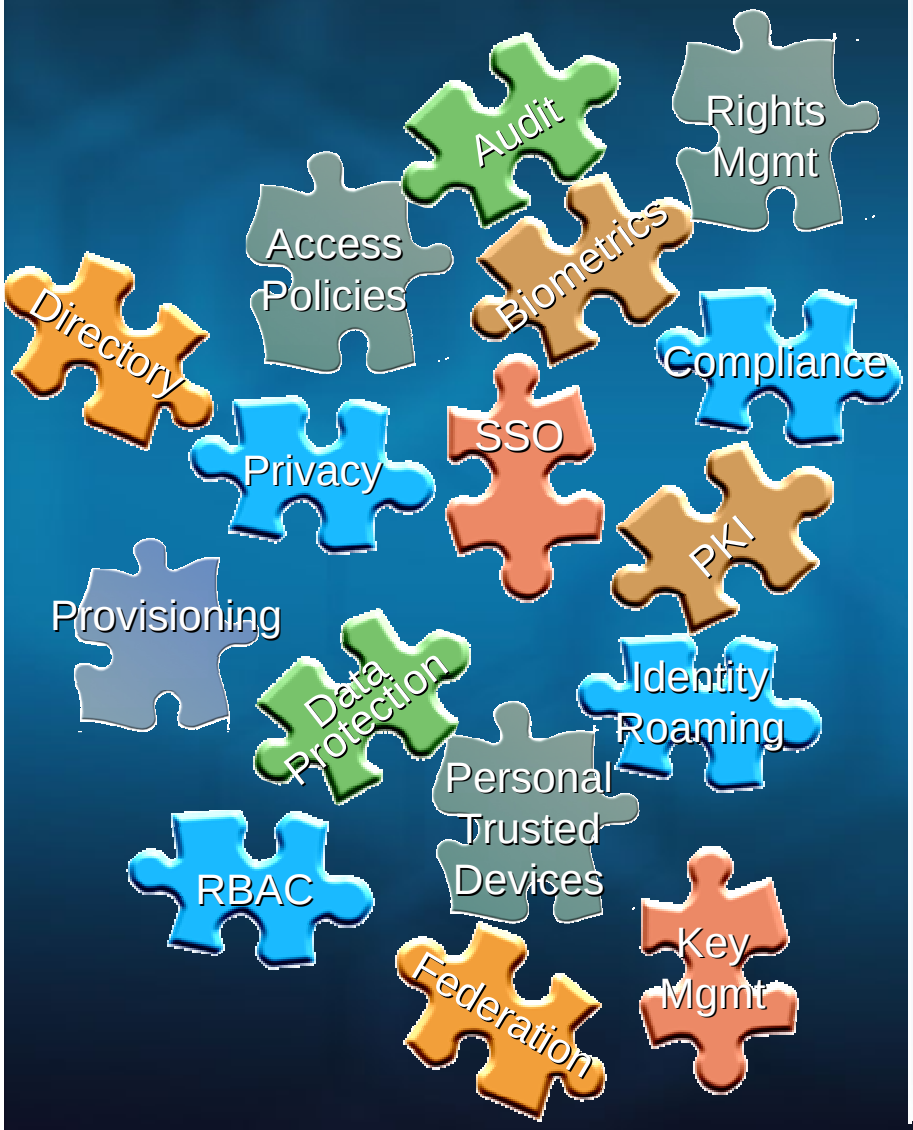
technologically-necessary principles of identity management

1. **User control and consent**
2. **Minimal disclosure for a defined use**
3. **Justifiable parties**
4. **Directional identity**
5. **Pluralism of operators and technologies**
6. **Human integration**
7. **Consistent experience across contexts**

Universal Identity Metasystem

- Allows digital identity to be loosely coupled:
  - multiple operators and implementations
  - connects existing and future identity systems
  - leverages the strengths of its constituent systems
  - provides interoperability between them
  - standards based
- Enables consistent and simple user experience

Critical Components of Identity Layer



- Identity Repositories
- Authentication
- Authorization
- Identity Federation
- Identity & Access Mgmt

Claims – “Currency” of Digital Identity

- ***Claim*** – assertion *in doubt*
- ***Fact*** – trusted claim
- Claims describe properties of *entities*:
  - *Subjects:* humans, devices, applications
  - *Resources:* services, devices, networks, data, transactions
  - *Actions:* resource-specific operations, e.g. read, approve
  - *Contexts:* runtime characteristics of access sessions
- ***Identity*** – context-specific set of Subject claims

Claims Taxonomy

- Identifier claims – unique entity markers in a given namespace

Subject Identifier Type	Strength
username	cognition
domain-specific identifier, e.g. account	directly controlled namespace
fully qualified domain name (FQDN)	hierarchical namespace
email address, phone #	client addressability, protocol non-ambiguity
URL	IdP addressability, protocol non-ambiguity
public key	“native” security

- Attribute claims – properties of an entity
  - Association claims – set membership descriptors of an entity
    - *Groups* – set of *Subjects*, e.g. “Manager”
    - *Capabilities* – set of *Resources/Actions*, e.g. “$50kPO/Approve”
    - *Scopes* – set of *Resources*, e.g. “Financial Report”
- Static claims, e.g. “DOB: May-21-1979”
- Derived claims, e.g. “AgeCategory: over-21”

Capability Claims

Capability - set of *Resources/Actions* to express:

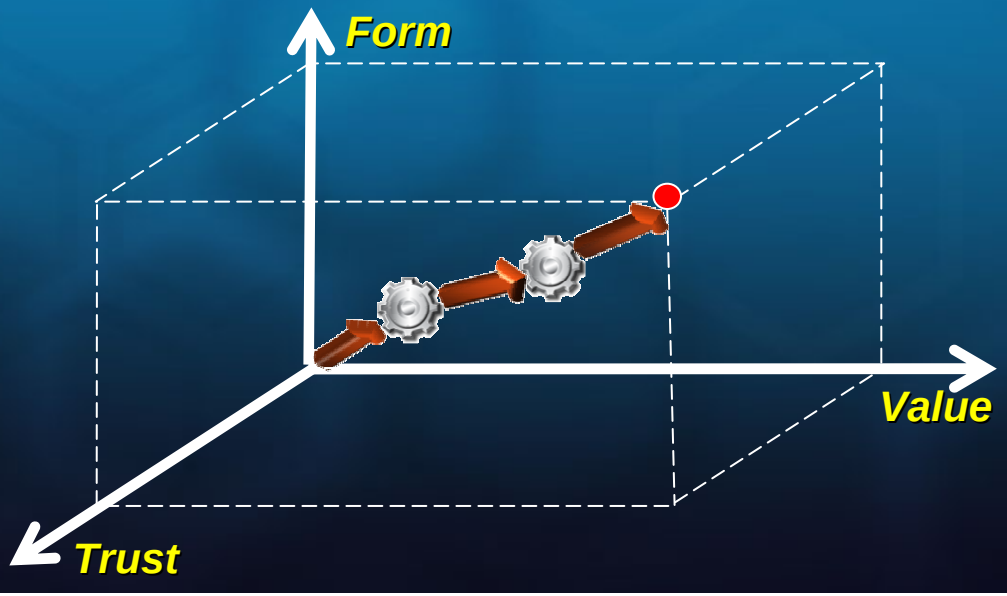
- Subject's *role* in Enterprise or Application
- Access *request*
- Access *grant*
- Unit of *delegation*

Capability Model	ACL Model
Explicit access grant	Implicit access grant via group membership
Separation of access decision and enforcement	Combined access decision and enforcement
Rich policy language (incl. delegation, SoD)	Constrained policy language
General purpose authorization model	Special-purpose: access to persisted objects
Scalable management due to separation of policies from resources	Hard to manage: highly distributed nature due to ACLs association with each resource

ACL – Access Control List
SoD – Separation of Duties

Claims Transformation

- Access process is a sequence of claim transformations
- Three dimensions of claims transformations:
  - ***Form:*** X.509 certificates ➡ SAML Assertions
  - ***Trust*****:** unsigned claims ➡ signed claims; claims ➡ facts
  - ***Value*****:** credentials ➡ attributes ➡ capabilities
- Transformation rules: *policies* describing claims relations
- Transformers: PKI Authorities, Token Services, directories, etc.
- Claims can be “pushed” to or “pulled” by transformers



Authentication

- Not an end in itself, part of the access process
- Distinct interactively-driven claim transformation step:
  - *trust/form* transform, e.g. username/password to SAML AuthN Statement
  - establishes level of confidence in the subject identity
  - establishes level of confidence of the subject real time presence
- Mutual (site-to-user) authentication
  - establishes level of confidence in the service identity
  - Authentication instrument: *credential = identifier claim + authenticator*

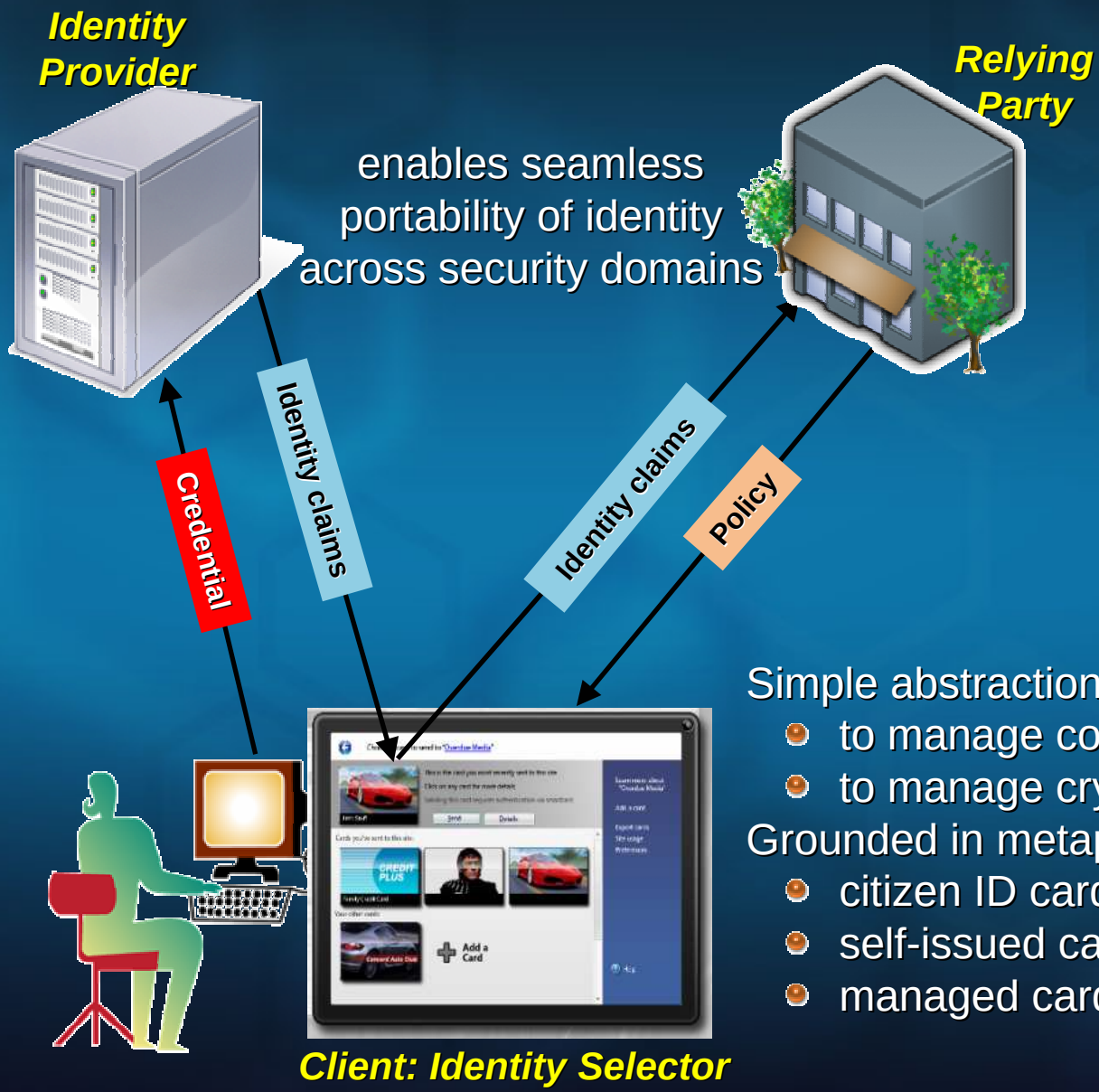
Identity Layer Authentication Facilities

- Pluggable multi-credential authentication framework
  - Credential collection: interactive solicitation of credentials
  - Credential validation: authenticator verification, claims transformation
  - Credential lifecycle management: provisioning, renewal, revocation
- Mutual authentication
- Advanced capabilities - transaction risk-based authentication

Personal Trusted Devices

- Authentication factors:
  - what you know – password, PIN
  - what you have - hardware token, Personal Trusted Device (PTD)
  - who you are – biometrics
  - hybrids, “grey areas”, e.g. RFID as biometric prosthesis ☺
- Goal: reduce over-reliance on password-based authentication
  - to increase level of confidence in subject’s identity
  - to combat phishing attacks through use of capture-resistant credentials
  - to enhance portability of identity claims
- Broad spectrum of PTDs – smart cards, OTP tokens, phones
- But there is a price:
  - cost of ownership
  - usability characteristics
  - management complexity
  - emergency access, e.g. scenarios when PTD is lost or unusable

Federated Identity



Simple abstraction of “digital personas”

- to manage collections of claims
- to manage cryptographic keys

Grounded in metaphor of physical cards

- citizen ID card, driver’s license, credit card
- self-issued cards signed by user
- managed cards signed by Identity Provider

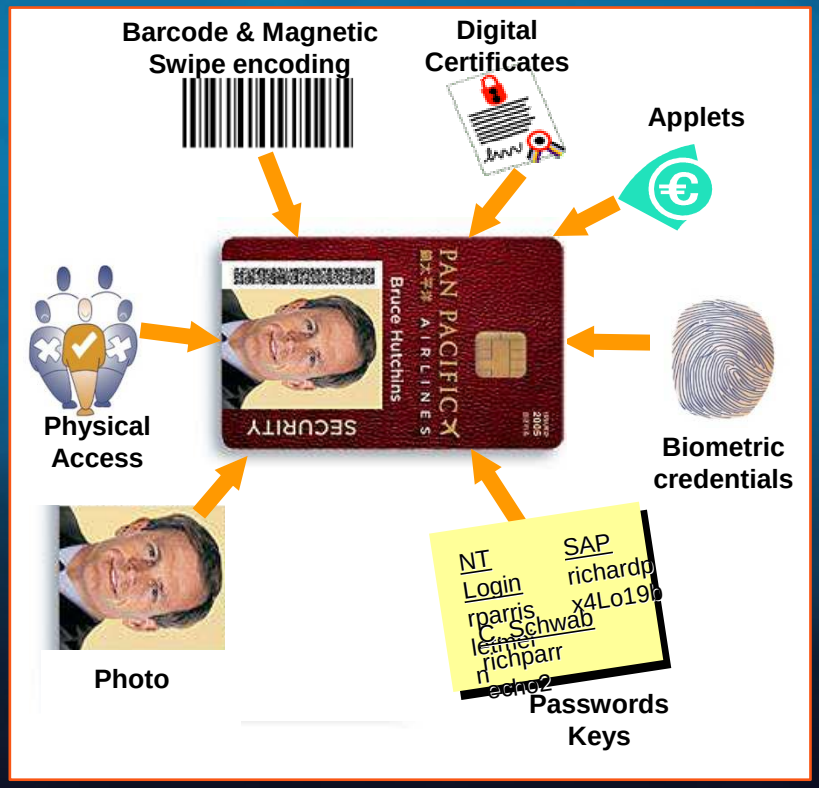
Privacy

- Privacy is woven throughout Laws of Identity
- Identity Metasystem based on these laws has privacy built-in, not add-on
  - empowers “user-centric” control of identity information
  - provides enhanced data protection for identity information
  - increases mutual trust and the level confidence for e-commerce

Identity and Access Management

Identity Layer management facilities for Identity:

- automated identity lifecycle management workflow
- delegation and self-service capabilities
- managing broad range of identity instruments, claims and access policies
- mechanisms for compliance with business and regulatory policies



Summary

Claims-based Identity Access and Management model

- enables common approach for building Internet Identity Layer
- establishes concept of claims as building blocks of Identity
- models access control as claim transformation process
- facilitates user-centric identity management and privacy
- enhances trust, usability and seamless nature of Identity