



International Telecommunication Union

Identity Management

Sergio Fiszman, Sr. Architect,
Nortel CTO organization, sergio@nortel.com



Ed Koehler, Sr. Architect,
Nortel Enterprise organization, ekoehler@nortel.com



Agenda



- o Problem Statements
- o Why is it important to address these problems?
- o The concept of identity management
- o Example - today vs. tomorrow
- o Goals

Problem Statements

e.g. End-User and Enterprise spaces

END USER

- **QoE:**
 - I have all these **IDs and passwords** – why can't my life be simpler and yet secure?
 - Every device is different – what do I do when I only have one device?
 - Every application I use asks me to log on and verify my credentials
- **Service Mobility:** What will happen when I **roam** across different networks and devices?
- **Trust:** Can I **trust** enterprises and service providers entities, **in a mobile world**?

ENTERPRISE

- **Regulatory:** Sarbanes-Oxley introduces new authentication and access control requirements.
- **OpEx:** How does identity management and autonomies save TCO money?
- **Supply-chain & e-Business:**
 - How can I control secure access to employees, contractors, suppliers, customers, ...?
 - How can I expand the boundaries of my enterprise services in a trusted manner?
- **Business Processes & Services:**
 - How can I **protect the enterprise assets**?
 - How can I **guarantee security assurance levels with more complex services**?

**Identity Management is all about trust and is the key to the end user.
It is the underpinning of security and autonomies.**



Why is it important to address these problems?

Problem

Expected Solution Results

- QoE: Many Ids and passwords → Reduces Cyber fraud and overall OpEx, while increasing end-user QoE
- Service Mobility → Increases end-user productivity
- Trust → Enables business growth & enterprise effectiveness
- Business Process & Services → Increases client loyalty
- Supply-chain & e-Business → Guarantees security assurance levels
- Regulatory compliance → Offers peace of mind, greater business agility, and reduces audit costs

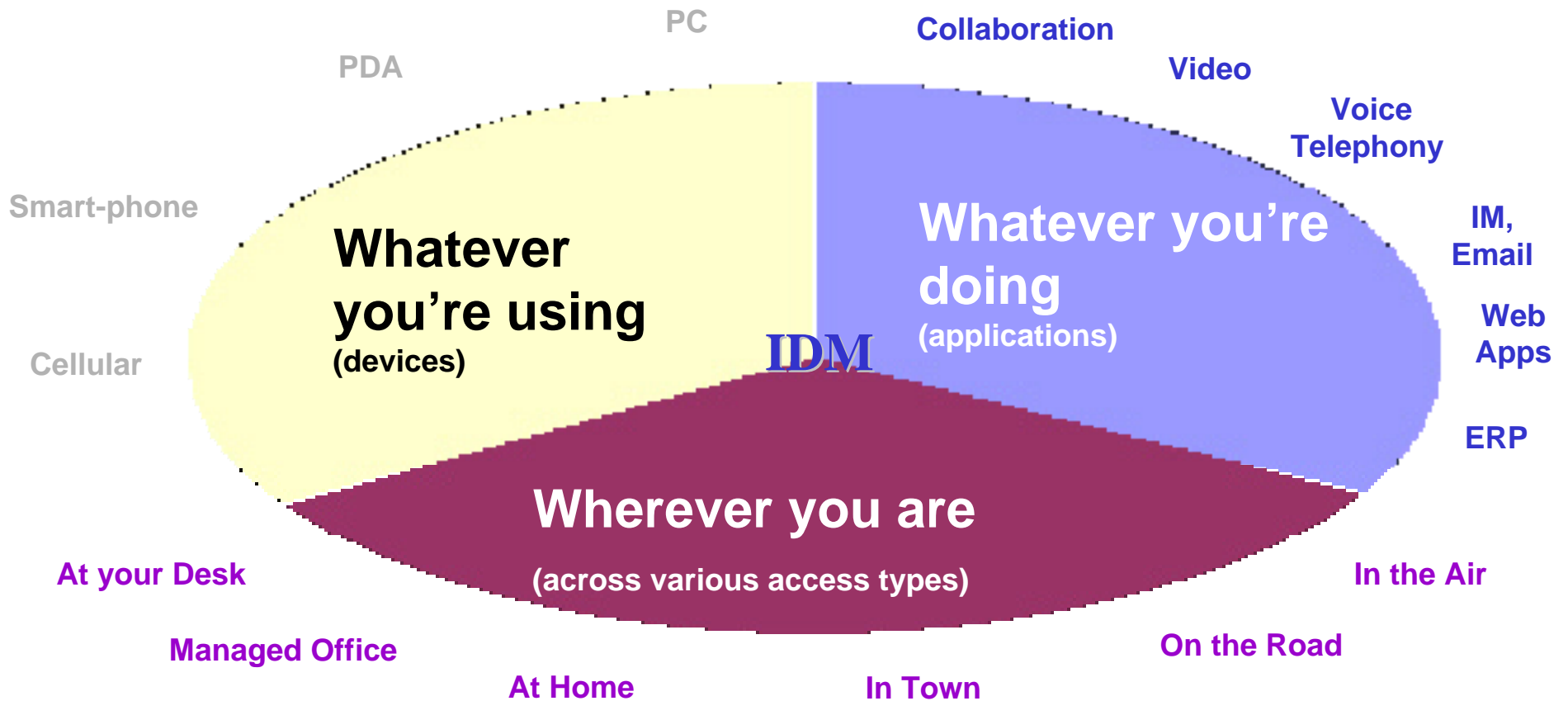


The Concept of Identity

Connecting users with services and with others (federation)

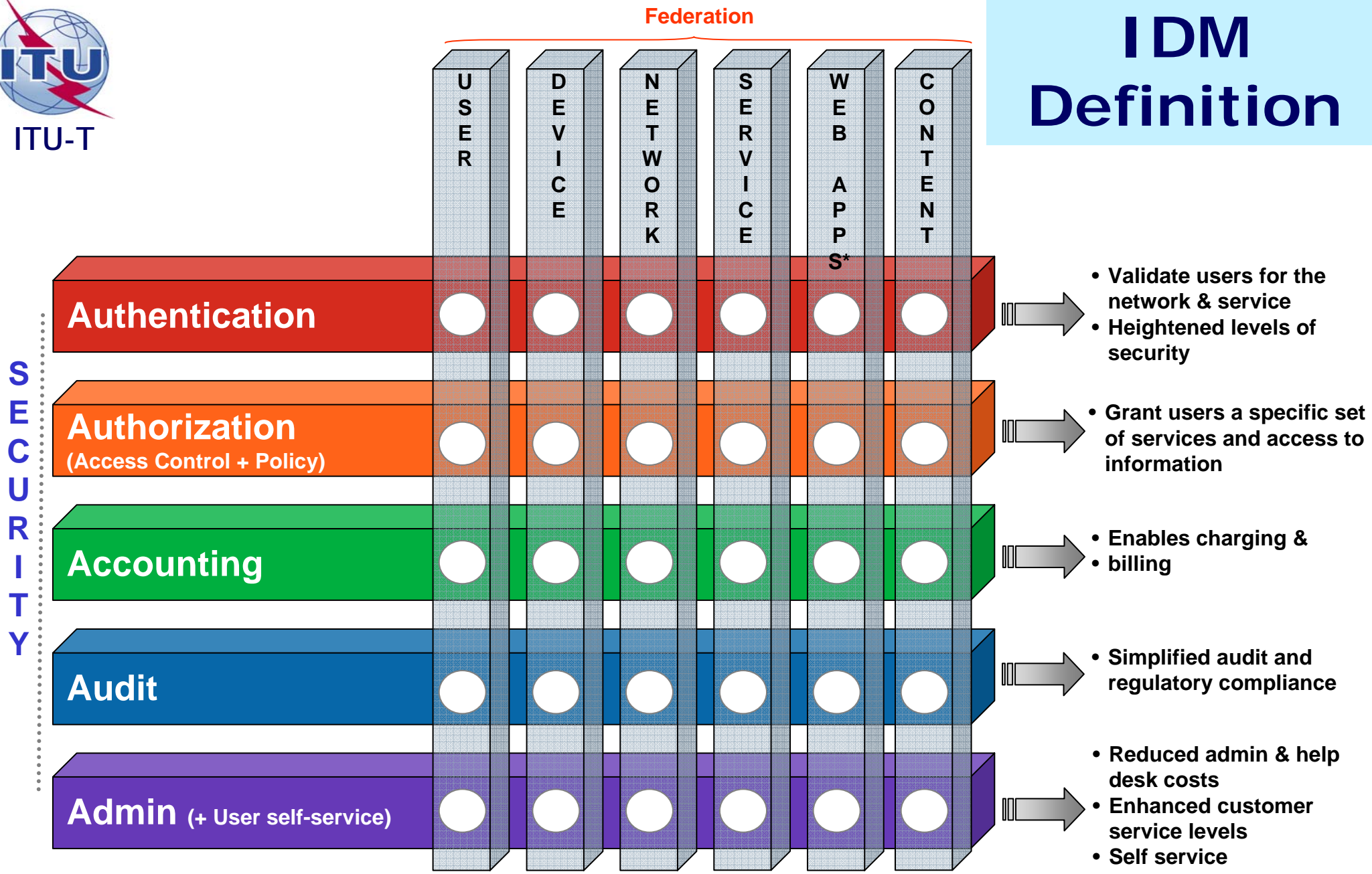
People have multiple identities

- Work – me@company.com
- Family – me@smith.family
- Hobby – me@icedevils.team
- Volunteer – me@association.org



Essential for trust & security and the operations of converged & virtual networks

IDM Definition



Example: Today versus Tomorrow

o Today

- Multiple Sign-on
- Single level of Assurance
- Protection is ad-hoc & manual
- Threat may not be contained and addressed in-time
- Tracking is partial. Too many ways to record interactions
- User-stickiness suffers
- High cost of ownership
- Mobility and Roaming is partial

o Tomorrow

- Reduced Sign-on
- Appropriate level of Assurance
- Protection is autonomic
- Threat addressed in a timely manner
- Tracking based on session-based auditing mechanisms
- User-stickiness is increased
- Lower cost of ownership
- Mobility and Roaming under federation of multiple networks and service providers

Goals

- A generic, open and context aware IDM solution that preserves the user identity, privacy and trust
 - Allows for secure mobility
- It works in any ecosystem
- It supports any business model
- It complements different federation methodologies

