Single Sign-On Architectures

Jan De Clercq

Senior Member of Technical Staff
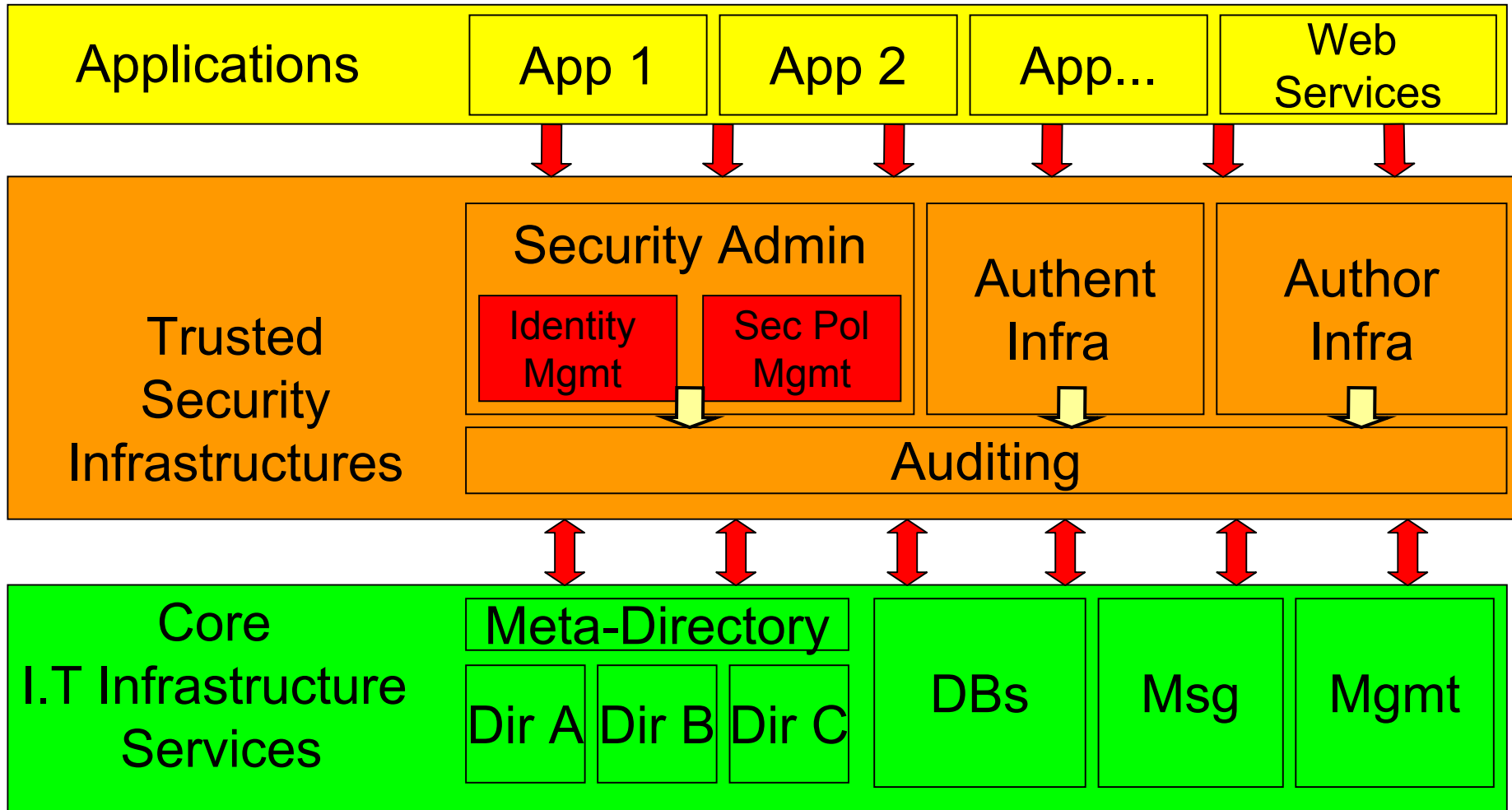Technology Leadership Group
Hewlett-Packard

Agenda

- Trusted Security Infrastructures

- SSO: What and Why?

- SSO Architectures

- Extending SSO
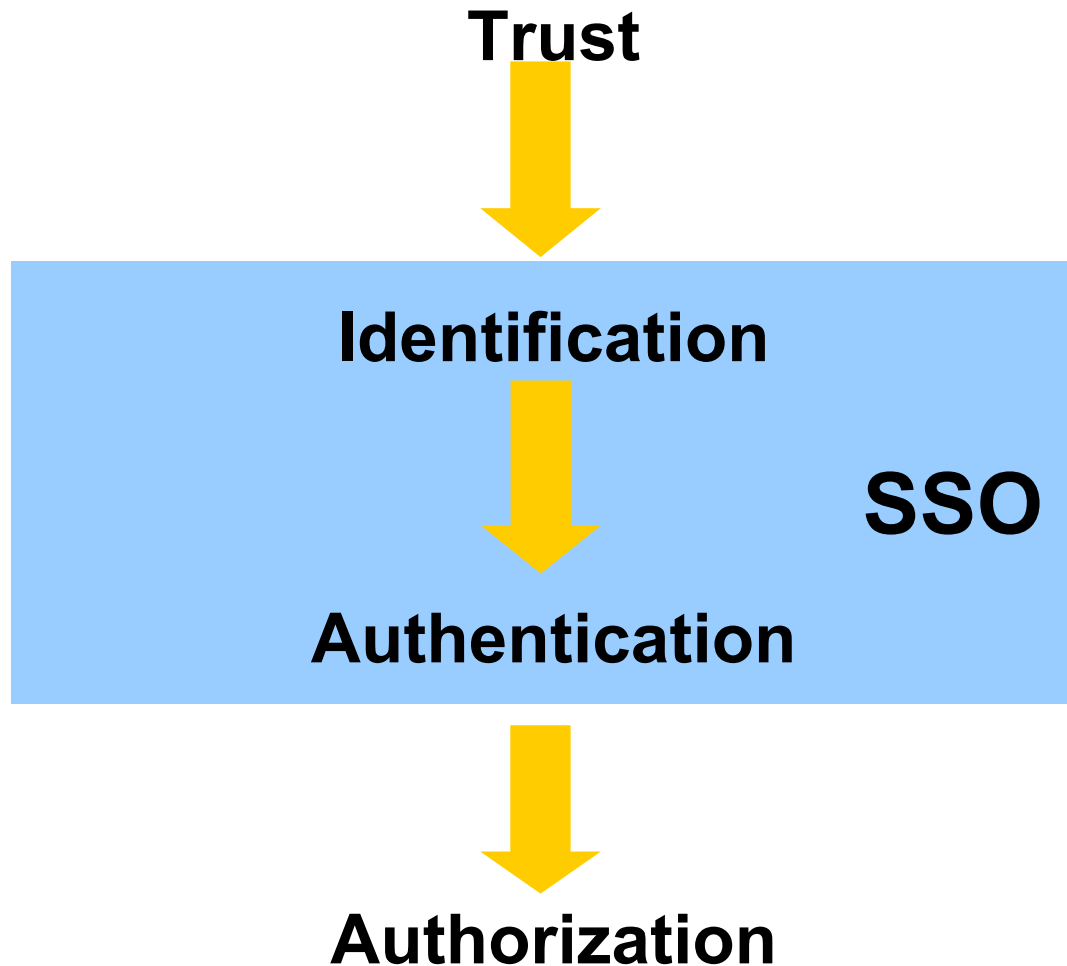
- Conclusion

Agenda

- **Trusted Security Infrastructures**

- SSO: What and Why?

- SSO Architectures

- Extending SSO

- Conclusion

Trusted Security Infrastructures (TSIs)

SSO Foundations: Trust

Trust

Identification

SSO

Authentication

Authorization

Agenda

- Trusted Security Infrastructures

- **SSO: What and Why?**

- SSO Architectures

- Extending SSO
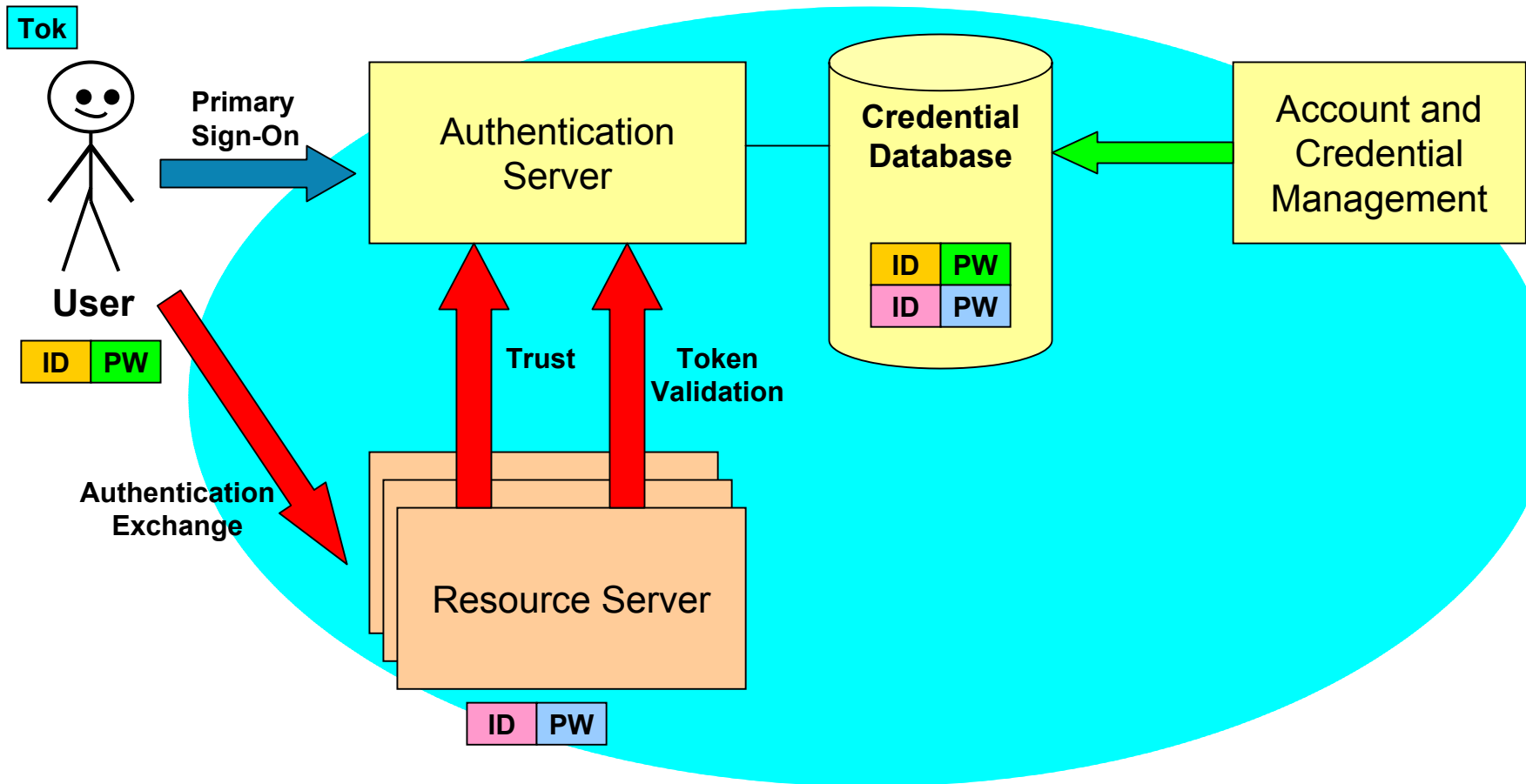
- Conclusion

SSO: What and Why?

- Ease of Administration

- Ease of Use

- Enables Enforcement of Coherent Security Policy

- Key to the Kingdom?

SSO Terminology

- Authentication Infrastructure
- Authentication Server
  - "Physical" providers of authentication/SSO
- Authentication Authority
  - "Logical" providers of authentication/SSO/Trust
    - = Domain (Windows speak)
    - = Cell (DCE speak)
    - = Realm (Kerberos speak)
- Authentication Credentials
- Digital Identity
- Credential Database
- Authentication Factors
- Authentication Token

SSO Terminology

Tok

User

ID PW

Primary Sign-On

Authentication Exchange

Authentication Server

Trust

Token Validation

Resource Server

ID PW

Credential Database

ID PW

ID PW

Account and Credential Management

Agenda

- Trusted Security Infrastructures

- SSO: What and Why?

- **SSO Architectures**

- Extending SSO

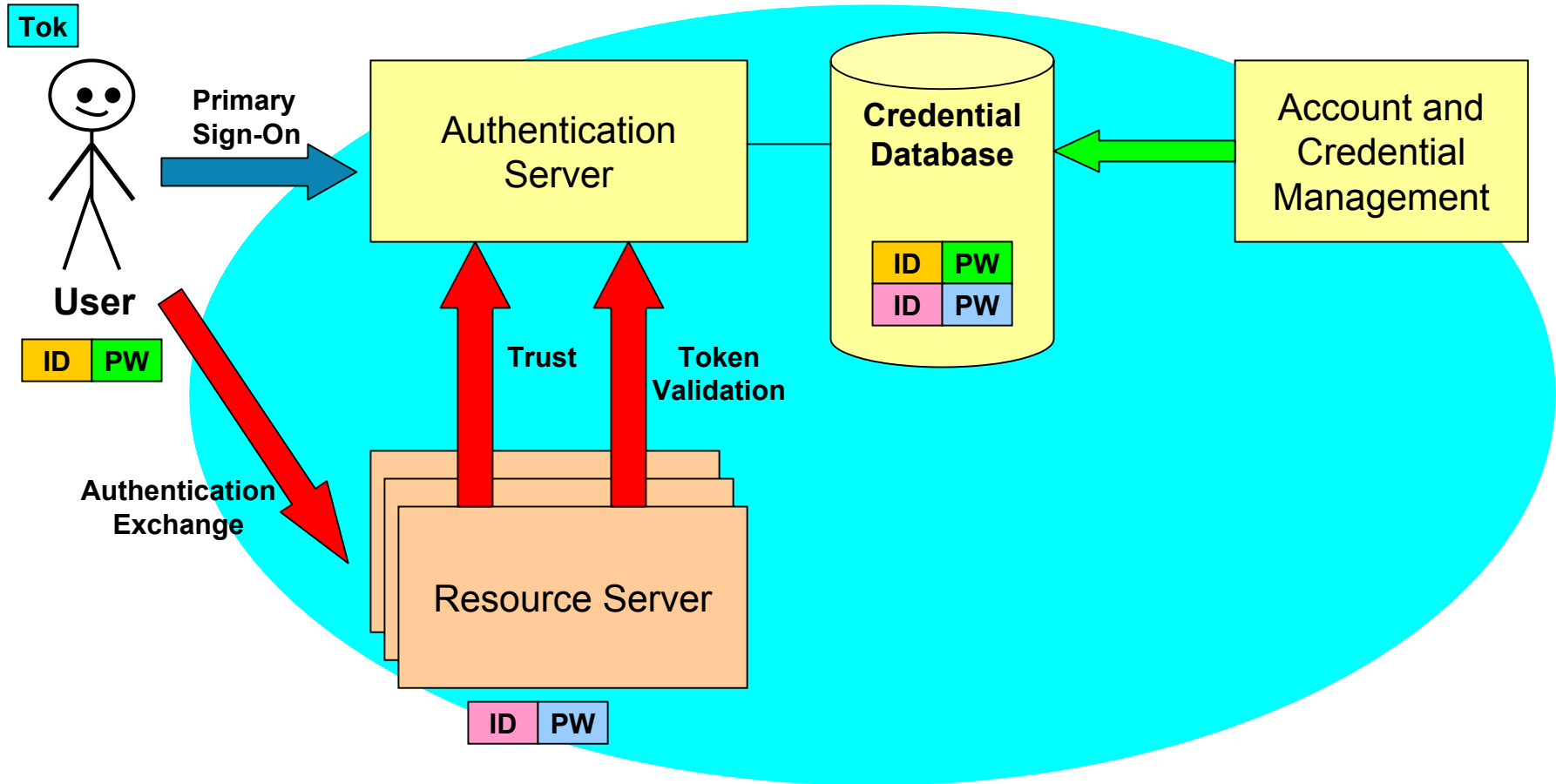- Conclusion

SSO Solutions and Architectures

- **Simple SSO**
  - Single Authentication Authority and Server
  - Single Authentication Authority and Multiple Servers
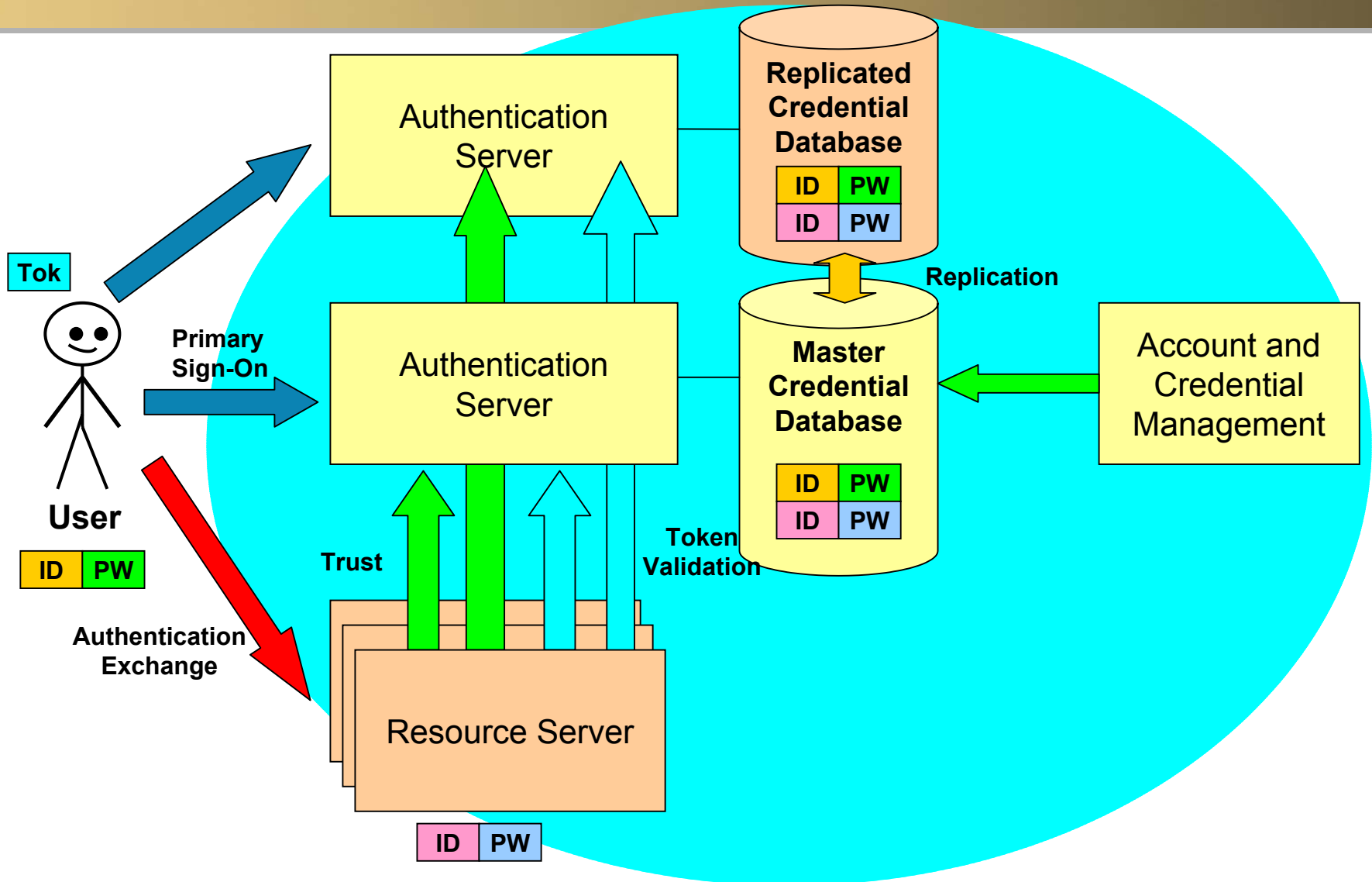
- **Complex SSO**
  - With Single Set of Credentials
    - Token-based SSO
    - PKI-based SSO
  - With Multiple Sets of Credentials
    - Credential Synchronization
    - Client-side Credential Caching
    - Server-side Credential Caching

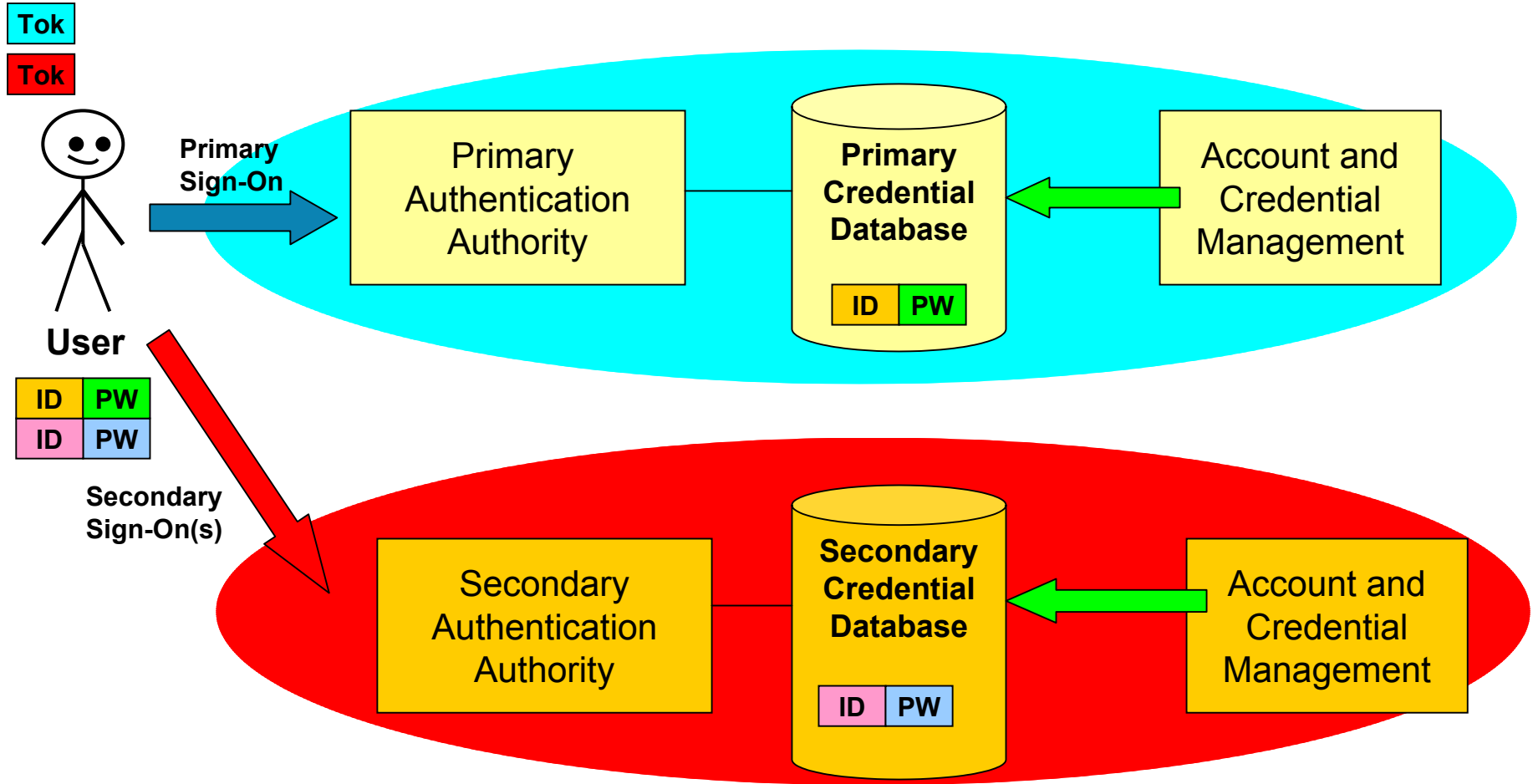# Simple SSO Solutions

Tok

User

ID PW

Primary Sign-On

Authentication Server

Credential Database

ID PW
ID PW

Account and Credential Management

Trust

Token Validation

Authentication Exchange

Resource Server

ID PW

Simple SSO Solutions

Traditional Sign-On (No SSO)

Tok

Tok

User

ID	PW
ID	PW

Primary Sign-On

Secondary Sign-On(s)

Primary Authentication Authority

Primary Credential Database

ID	PW

Account and Credential Management

Secondary Authentication Authority

Secondary Credential Database

ID	PW

Account and Credential Management

Complex SSO Solutions: Single Credential Set: Token-based SSO

Primary Sign-On

Temporary Token

Tok

User

ID | PW

Transparent Secondary Sign-On(s) using Temporary Token

ID | PW

Primary Authentication Authority

Primary Credential Database

ID | PW
ID | PW

Account and Credential Management

Trust

Secondary Authentication Authority

Secondary Credential Database

Account and Credential Management
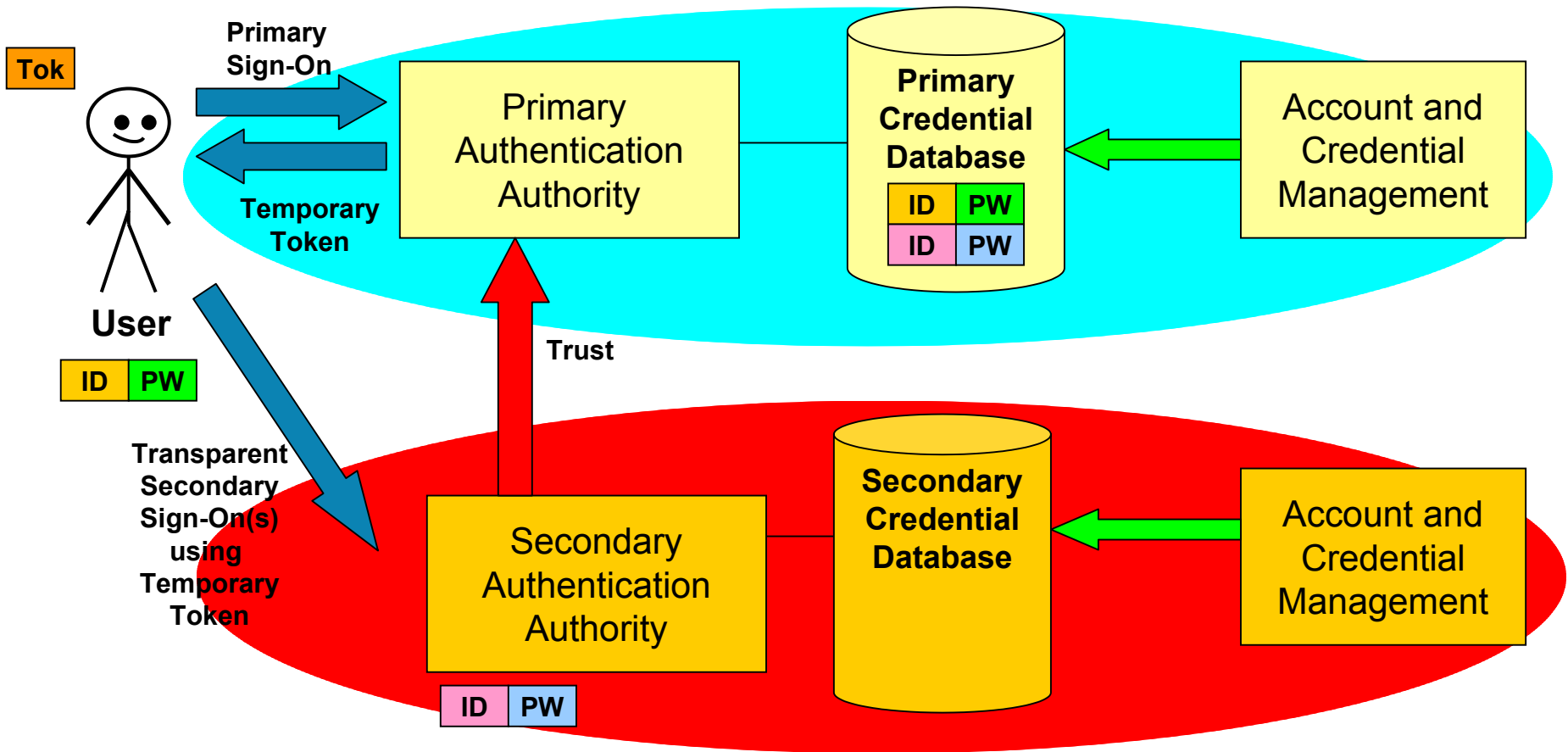
Complex SSO Solutions: Single Credential Set: PKI-based SSO

ID **PW**

User Registration

User Private Key

User

User Cert

CA Cert

Certificate Issuance

Transparent Secondary Sign-On(s) using Public Key Credentials (Certificate and Private Key)

Primary Authentication Authority

CA Cert

Trust

Secondary Authentication Authority

CA Cert

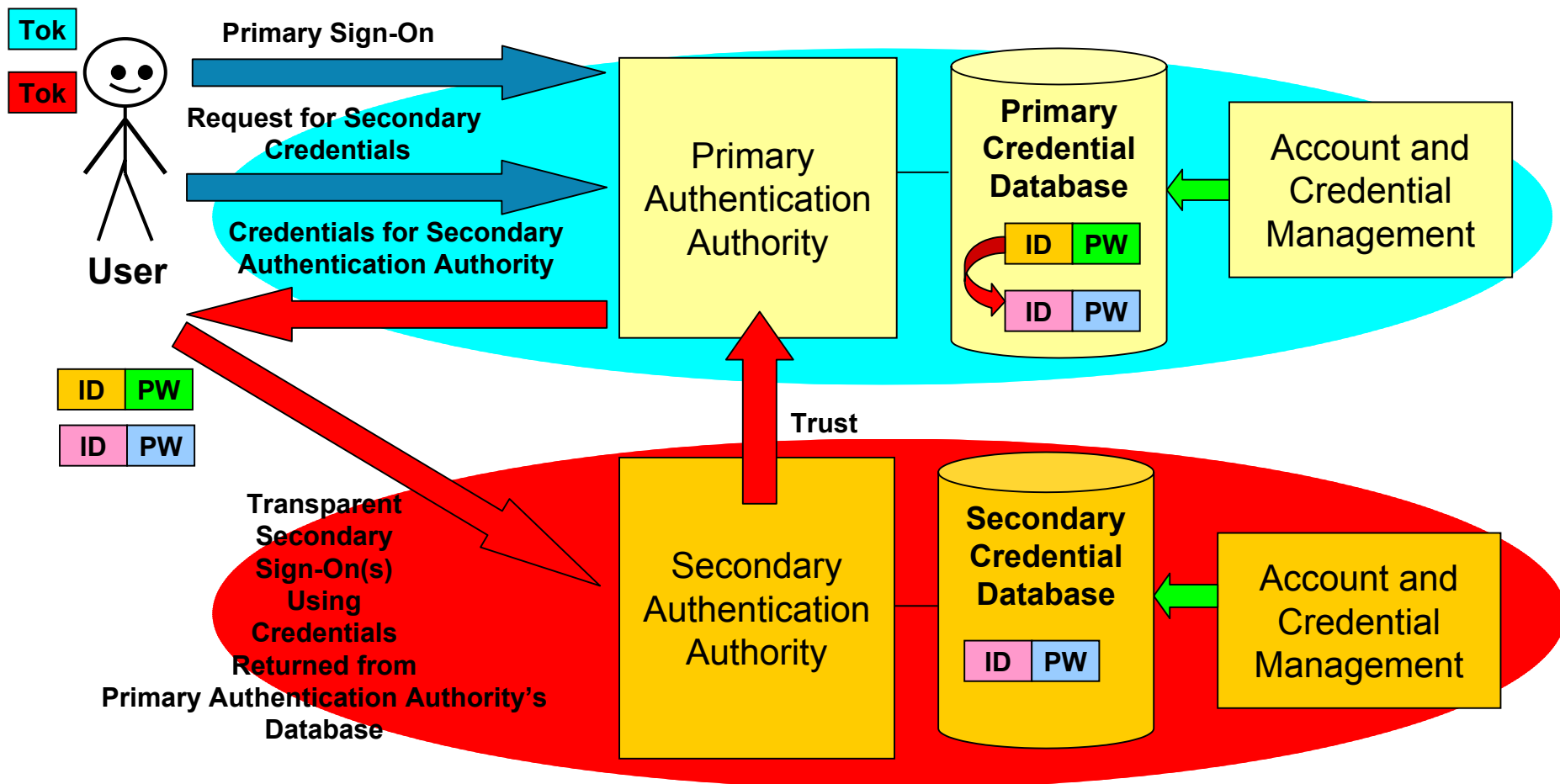**Credential Database**

ID **PW**

Account and Credential Management
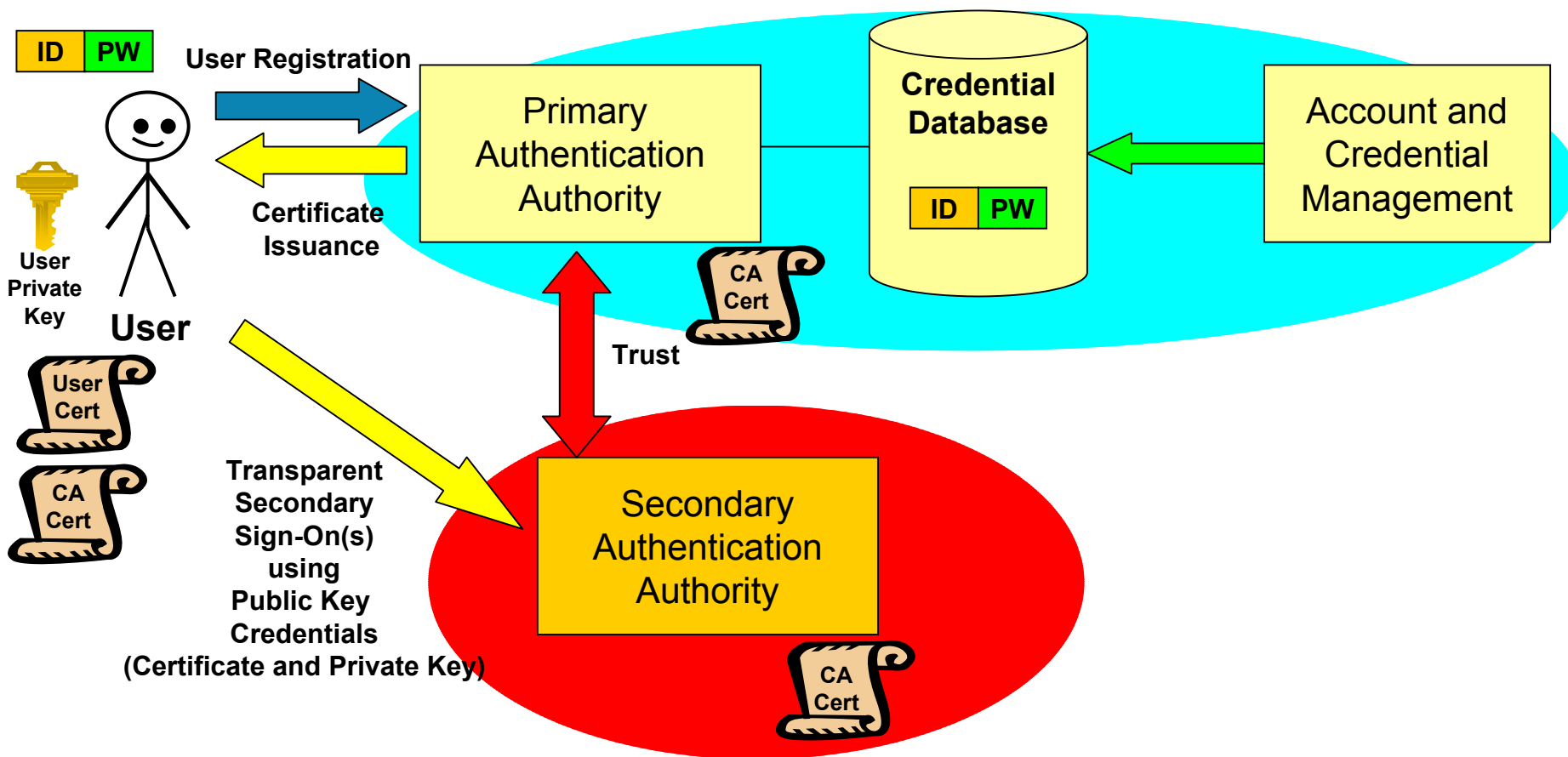
Complex SSO Solutions: Multiple Credential Set: Password Sync
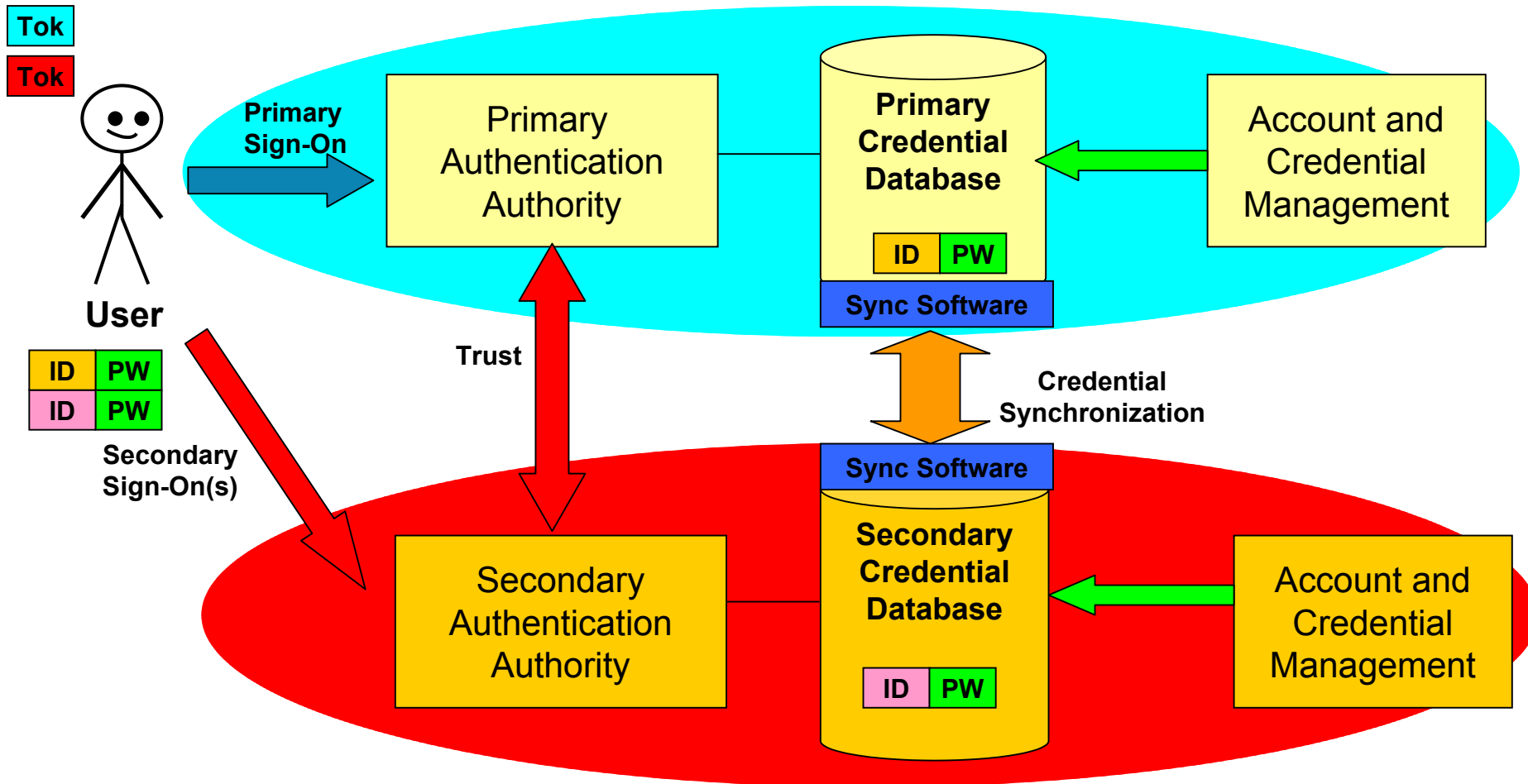
Complex SSO Solutions: Multiple Credential Set: Client-side Caching

Tok
Tok
PW

User

Primary Sign-On

Primary Authentication Authority

Primary Credential Database

ID **PW**

Account and Credential Management

Secure Client-Side Credential Cache

PW
ID **PW**
ID **PW**

Trust

Transparent Secondary Sign-On(s) Using Cached Credentials

Secondary Authentication Authority

Secondary Credential Database

ID **PW**

Account and Credential Management
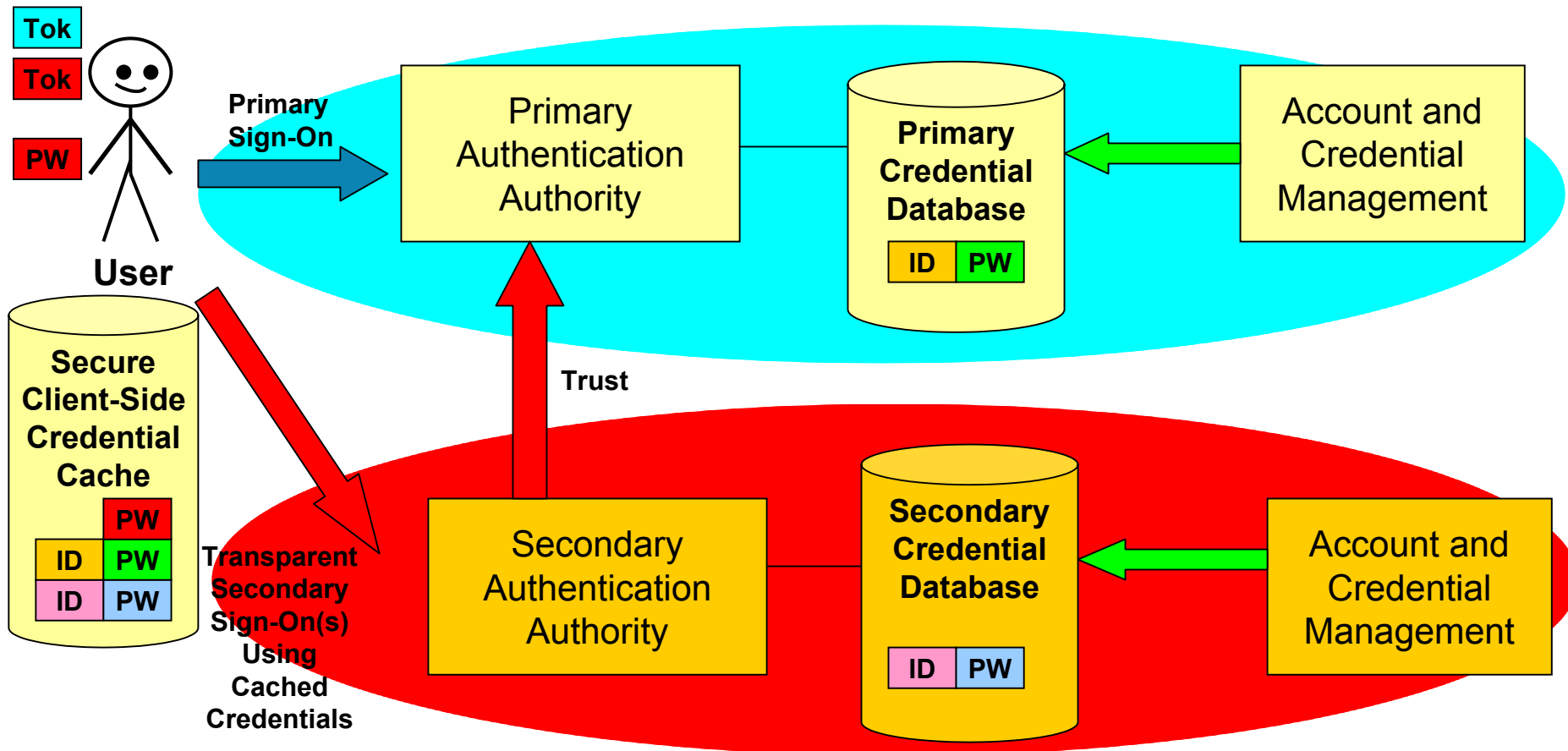
Complex SSO Solutions: Multiple Credential Set: Server-side Cache

Agenda

- Trusted Security Infrastructures

- SSO: What and Why?

- SSO Architectures

- **Extending SSO**

- Conclusion

Extending SSO

- **To cover Different Organizations**
  - Scope: Extranet and Internet
  - "Federation"

Defining Federation

" The Use of agreements, standards, and technologies to make identity and entitlements portable across autonomous identity domains."

Extending SSO: Federation

	Kerberos-based federation	PKI-based federation	SAML-based federation
Authentication Technology	Kerberos	PKI	Any
Platform support	Many	Many	Many
Support for entity authentication	Yes	Yes	Yes
Support for data authentication	No	Yes	Under development
Authorization Federation Support	Yes, but not standardized	Yes, but very few products support it	Yes
Granularity of trust relationship and security policy support	Very Monolithic, no policy support	Support for granular trust and security policies in some products	Under development
Status	Standardized	Standardized, though standardization is not complete	Under development

Agenda

- Trusted Security Infrastructures

- SSO: What and Why?

- SSO Architectures

- Extending SSO

- **Conclusion**

Conclusion

- Creating an SSO Infrastructure for a heterogeneous environment is not an easy job

- The creation of SSO Infrastructures is a great opportunity to leverage directory and meta-directory investment

- Prefer open standards above proprietary solutions

- Keep it simple

Overview

- Trusted Security Infrastructures

- SSO: What and Why?

- SSO Architectures

- Extending SSO

- Conclusion

Questions?

- Jan.DeClercq@HP.com

Interex, Encompass and HP bring you a powerful new HP World.