

# **Single sign-on (SSO)**

Presentation

Tiit Erm

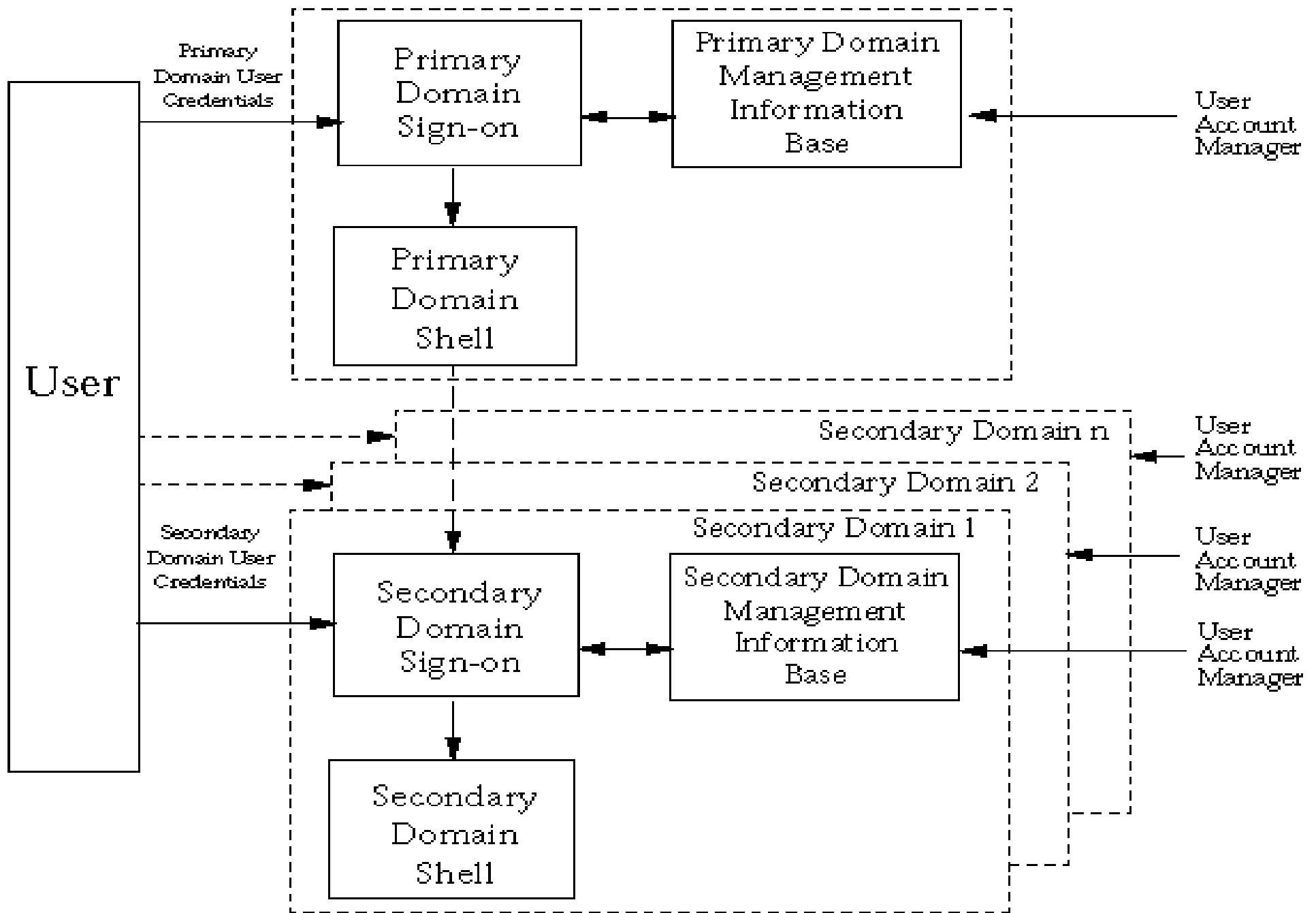
106572 IVCMM

# Main points

- Introduction
  - Old approach in multiple systems
  - SSO
- Security
- Benefits
- Common SSO based configurations
- Examples of SSO usage
- Conclusion

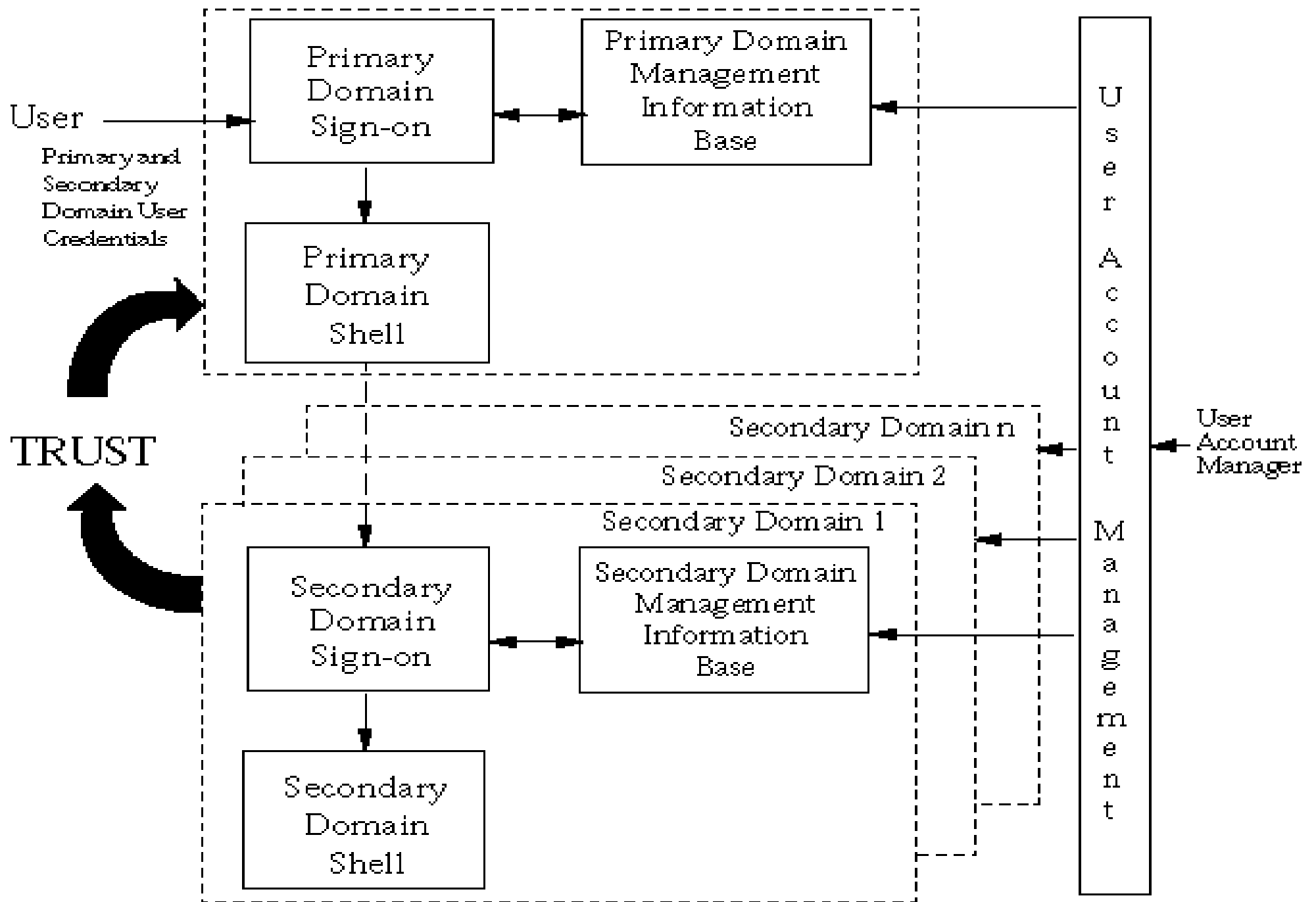
# Introduction – old approach

- Multiple/distributed systems -> multiple sign-on dialogues -> multiple usernames and passwords
- We have:
  - Distributed system – independent security domains
  - N domains, N platforms, N accounts, N account managers ->
  - Complicated schema:  
[http://www.opengroup.org/security/sso/sso\\_intro.htm](http://www.opengroup.org/security/sso/sso_intro.htm)



# SSO

- Single sign-on: multiple related, independent systems – user logs into once and gains access to all systems
- Single sign-off: single action of signing out terminates access to multiple systems
- Not so complicated schema:  
[http://www.opengroup.org/security/sso/sso\\_intro.htm](http://www.opengroup.org/security/sso/sso_intro.htm)



# Security aspects

- **Secondary domains have to trust the primary domain to:**
  - **correctly assert the identity and authentication credentials of the end user,**
  - **protect the authentication credentials used to verify the end user identity** to the secondary domain from unauthorised use.
- **The authentication credentials have to be protected when transferred between the primary and secondary domains** against threats arising from interception or eavsdropping leading to possible masquerade attacks.

# System requirements

- Increased focus on user credentials
  - Strong authentication methods: Smart cards, one-time passwords
- Authentication systems are critical value to company
  - Not good for systems which access must be need guaranteed at all times (i.e security systems)

# Benefits

- **Reduces phishing success**, because users are not trained to enter password everywhere without thinking.
- **Reducing password fatigue** from different user name and password combinations
- **Reducing time** spent re-entering passwords for the same identity
- Can support conventional authentication such as Windows credentials (i.e., username/password)
- **Reducing IT costs** due to lower number of IT help desk calls about passwords
- **Reduction in the time taken**, and **improved response**, by **system administrators in adding and removing users** to the system **or modifying their access rights**
- **improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration** including the ability to inhibit or remove an individual user's access to all system resources in a co-ordinated and consistent manner.

# Benefits

- **Security on all levels** of entry/exit/access to systems **without the inconvenience of re-prompting users**
- **Centralized reporting** for compliance adherence.


# Common SSO based configurations

- Kerberos based
  - Kerberos ticket-granting ticket (TGT)
- Smart Card based
- OTP Token
  - Password sent via SMS
- Integrated Windows Authentication
  - MS Internet Information Services and IE

# Examples of SSO usage

- FaceBook Platform – APIs interact with FB features
- OpenAM (OpenSSO)
- Ubuntu SSO – Launchpad, Ubuntu One, Ubuntu shop, etc
- Windows Live ID
  - Hotmail, Messenger, Xbox Live



One Windows Live ID gets you into **Hotmail, Messenger, Xbox LIVE** — and other places you see 

### Sign up


Windows Live ID gives you access to Microsoft services including MSN, Hotmail, Office Live, Xbox LIVE, and many more.

Don't have a Windows Live ID?

[Sign up](#)

[More about Windows Live ID](#)

### Sign in

 Windows Live ID:   
(example555@hotmail.com)

Password:

[Forgot your password?](#)

Remember me on this computer (?)

Remember my password (?)

[Sign in](#)

Use enhanced security

# Conclusion

- Useful for multiple (distributed) systems
- Strong authentication needed
- User and administrator friendly
- Reduces time and IT costs
- Improved security level

Thank you for your attention!  
Questions?

# References

- Introduction to Single Sign-On (opengroup.org):  
[http://www.opengroup.org/security/sso/sso\\_intro.htm](http://www.opengroup.org/security/sso/sso_intro.htm)
- Single sign-on (wikipedia.org):  
[http://en.wikipedia.org/wiki/Single\\_sign-on](http://en.wikipedia.org/wiki/Single_sign-on)
- Facebook Connect (wikipedia.org):  
[http://en.wikipedia.org/wiki/Facebook\\_connect#Facebook](http://en.wikipedia.org/wiki/Facebook_connect#Facebook)