




# Designing Key Management with Usability in Mind

Mary Theofanos  
Brian Stanton



ISO 9241-210:2010

“Usability: The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.”

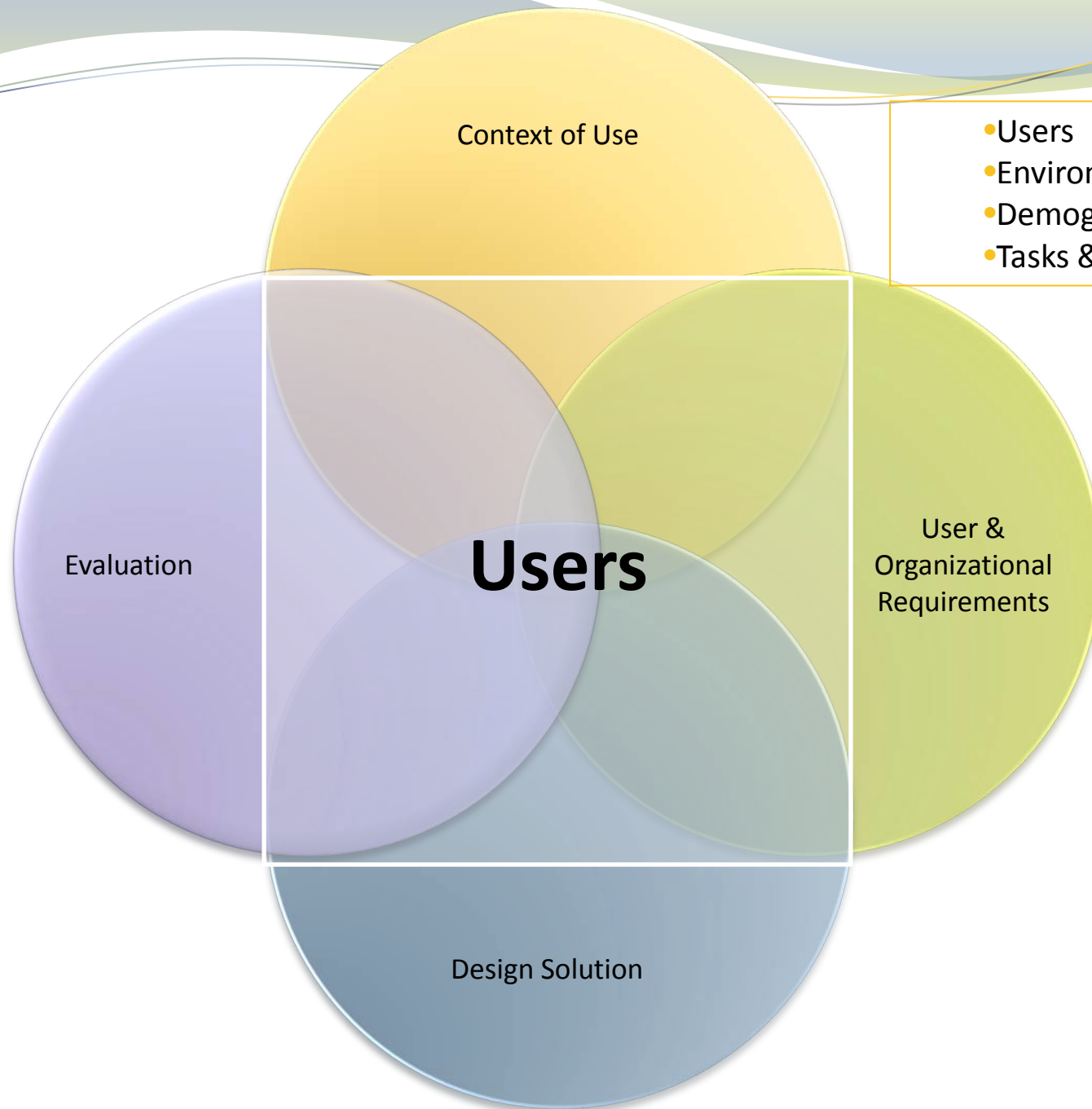
Effectiveness: a quality metric (errors, accuracy )  
How well can the product be used?

Efficiency: What the user has to do – time to complete a task

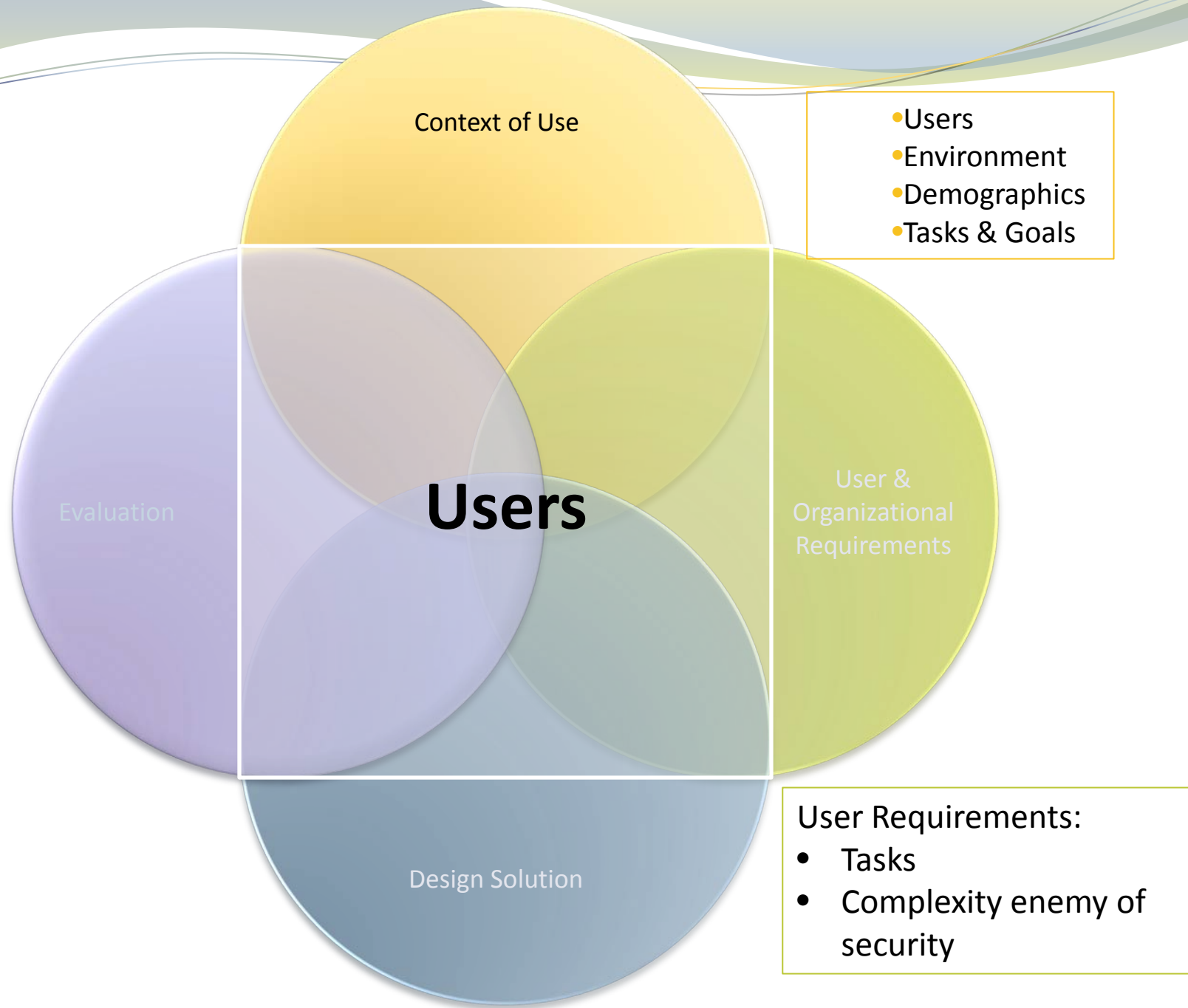
Satisfaction: How the user feels about the product (comfort, frustration)

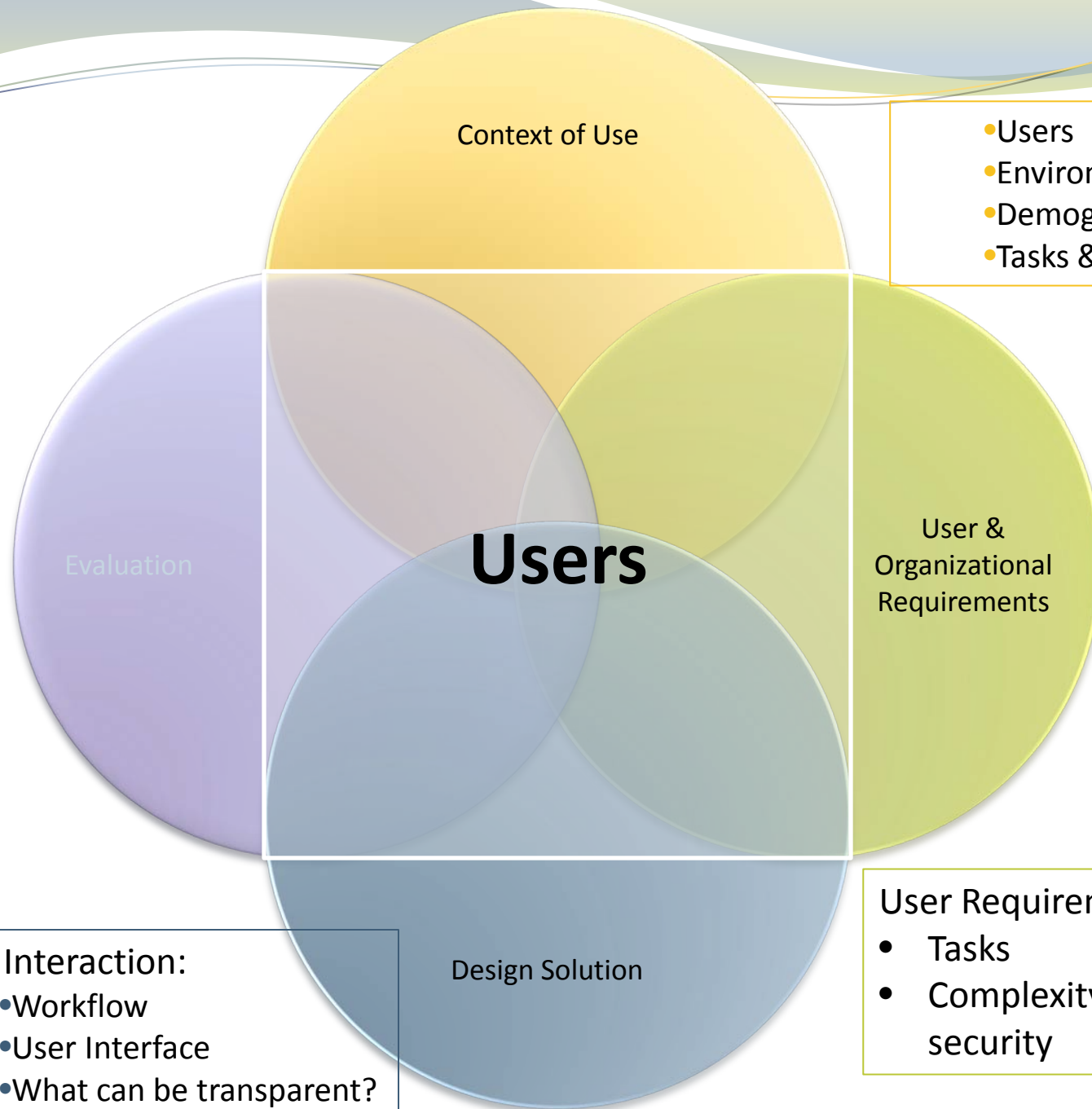


context of use



- Users
- Environment
- Demographics
- Tasks & Goals





- Users
- Environment
- Demographics
- Tasks & Goals

#### User Interaction:

- Workflow
- User Interface
- What can be transparent?

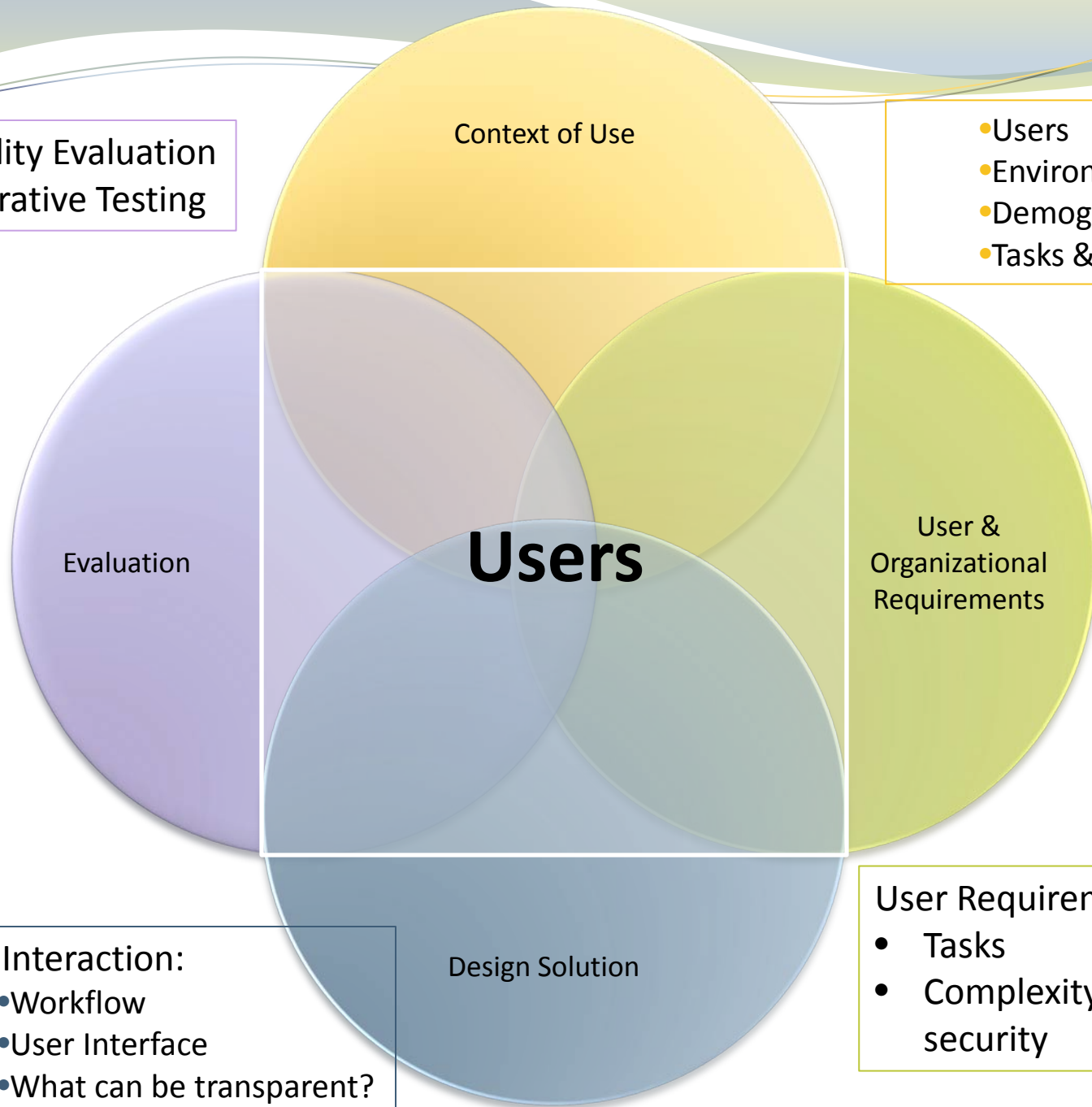
#### User Requirements:

- Tasks
- Complexity enemy of security

Usability Evaluation

- Iterative Testing

- Users
- Environment
- Demographics
- Tasks & Goals



User Interaction:

- Workflow
- User Interface
- What can be transparent?

User Requirements:

- Tasks
- Complexity enemy of security

# Case Study 1: PKI Deployment for an Enterprise Wireless Network

## Palo Alto Research Center (PARC)

- Idea was to give 200 users an X.509 certificate and to use 802.1x Extensible Authentication Protocol in TLS mode to authenticate to the wireless network
  - Request and retrieve certificates through web-based interface
  - Configure through GUI-based 802.1x configuration software
  - Administrators provided set of detailed instructions



## And the result

Studied 8 users (Ph.D.'s in Computer Science):

- Process involved 38 distinct steps
- Average time to request, receive certificate, and configure system 140 minutes
- Almost all followed the instructions mechanically
- Many described enrollment as most difficult computer task ever been asked to do
- All had little idea of what they had done to their machines
- Reduced their ability to configure and maintain their own machines.

## Solution:

### Usable PKI Deployment for Wireless Network


- Automated PKI and CA setup
- Enrollment Station is locked in room
  - Intuitive trust model
  - User and user's badge
  - Context of use
- Studies shows take 1minute 39 secs
- Total of 4 steps to add new device, retrieve certificate and install for use with the wireless network
- Positive user satisfaction and confidence

# Case Study 2: NIST PIV Pilot

100 Pilot users (26 usability users ) over 10 weeks used the PIV card and pin to:

- Log in to their computer
- Digitally sign email
- Encrypt email
- Access a web application to register visitors





# Start-up process was designed to be straight forward:

1. Update certificates on PIV badge
2. Card reader installation/ smartcard middleware
3. User training and documentation


# What did we learn?

- One size does not fit all. A wide range of devices should be evaluated and be made available for users to choose
- Continue to support use of username and passwords to address forgotten, stolen and lost PIV cards.
- Refrain from mandating a PIN that changes frequently
- No clear policy on when to encrypt/decrypt or digitally sign an email
- Clear guidance on how to choose between certificates.
- How do you use PIV for multiple computers at one time
- All web applications should use PIV

# Users Views of PIV Security

- Users develop mental models of security that are inaccurate
  - No concept that possessing the card is part of the overall security mechanism (multi-factor)

Reinforces the importance to maximize direct benefits to users because security is not what drives the users



We learned this specifically because we performed testing and ran the pilot!

We were able to learn about and know our users through:

- Daily emails surveys (diary)
- Periodic interviews
- Direct observation
- Pre and post surveys

and questions like:

Did you use the PV card to login today?

If not why not?

Did you have problems?

# First Tenet: Know Thy User – don't wait for Pilot

## Basis for User Requirements

- Users' characteristics – who is your user?
- Users are task driven – what is their primary task?
- What is their mental model?  
In general we have found that users' understanding of security is weak
  - Can they explain certificates or PKI?
- Users' perception (because these influence their behavior)
  - Do they believe there are impossible demands
  - Are they looking for direct benefit
  - Are things too complex in their eyes



## 2<sup>nd</sup> Tenet: Test Early – Test Often

Testing ranges from simple to complex

- A simple questionnaire can address terminology and definitions
- Paper prototyping can investigate workflow and user interfaces
- Even usability testing can be used incrementally on phased development to test components.
- Finally pilots can test entire systems

# User Requirements and Usability Testing Can:

1. Make it easy for users to do the right thing!
  - ▶ Definition of usability: users, goals, context of use
2. Align to the users conceptual model
  - ▶ Defining some of the terms on the interface differently
3. Reduce the complexity for the user
4. Eliminate those factors which inhibit adoption of Key management systems and encourage those that factors that promote adoption