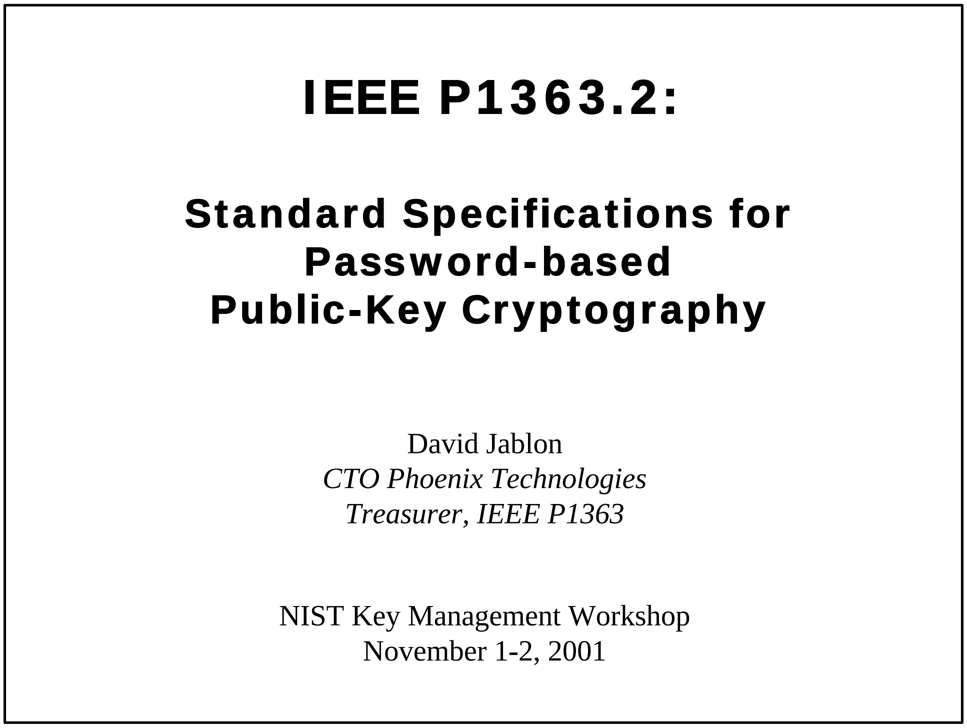
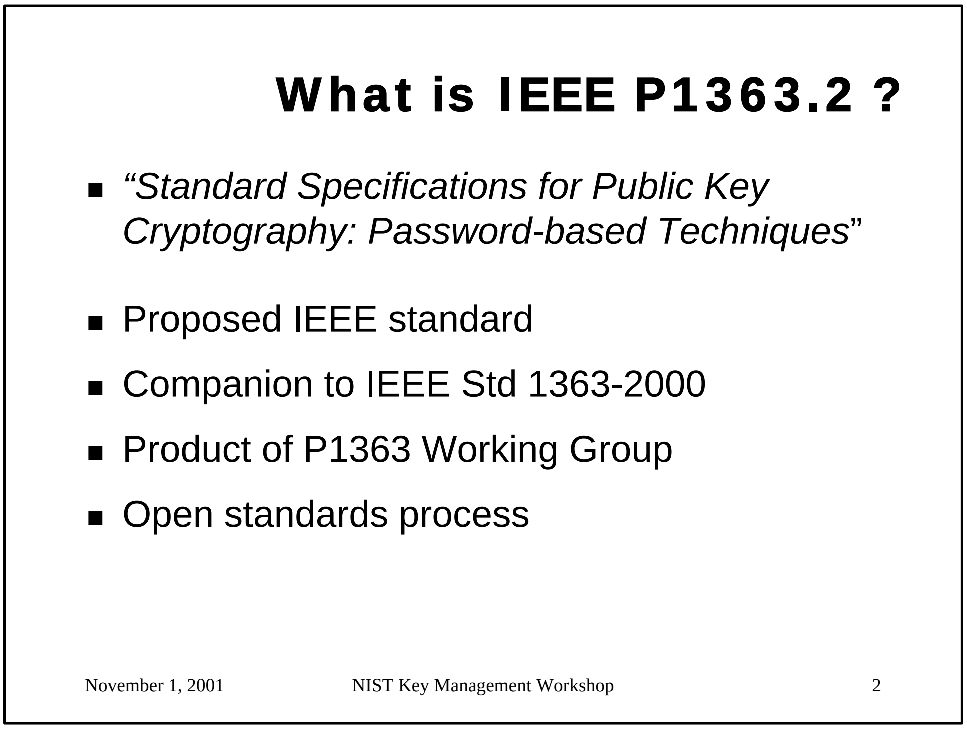


# IEEE P1363.2:

## Standard Specifications for Password-based Public-Key Cryptography

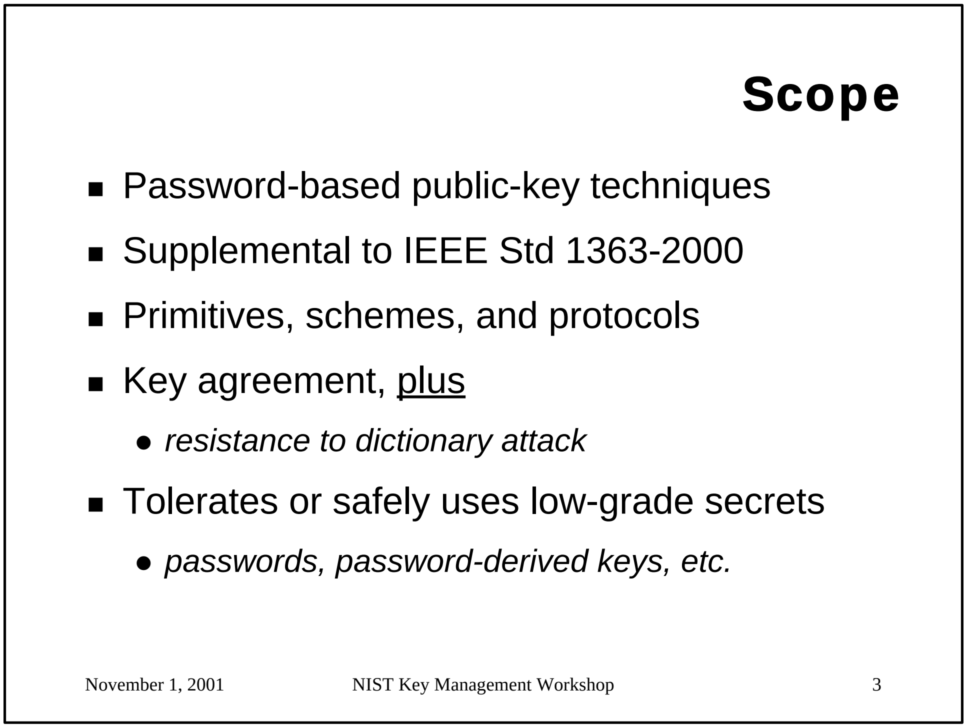
David Jablon
*CTO Phoenix Technologies*
*Treasurer, IEEE P1363*

NIST Key Management Workshop
November 1-2, 2001



## What is IEEE P1363.2 ?

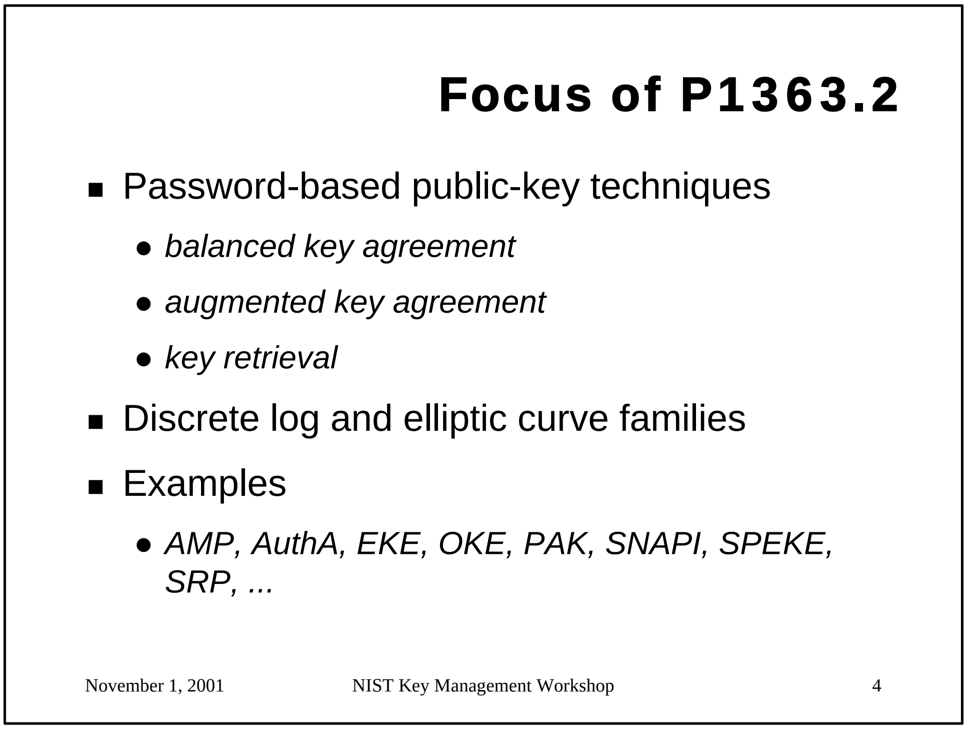
- *"Standard Specifications for Public Key Cryptography: Password-based Techniques*"
- Proposed IEEE standard
- Companion to IEEE Std 1363-2000
- Product of P1363 Working Group
- Open standards process



## Scope

- Password-based public-key techniques
- Supplemental to IEEE Std 1363-2000
- Primitives, schemes, and protocols
- Key agreement, plus
  - *resistance to dictionary attack*
- Tolerates or safely uses low-grade secrets
  - *passwords, password-derived keys, etc.*

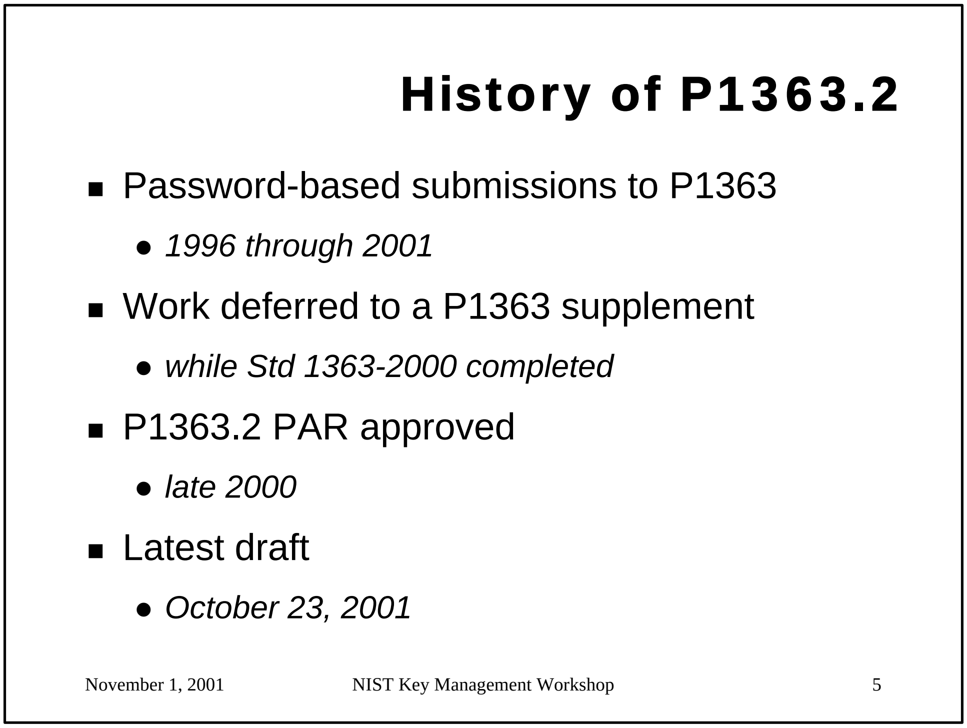
November 1, 2001 NIST Key Management Workshop 3



## Focus of P1363.2

- Password-based public-key techniques
  - *balanced key agreement*
  - *augmented key agreement*
  - *key retrieval*
- Discrete log and elliptic curve families
- Examples
  - *AMP, AuthA, EKE, OKE, PAK, SNAPI, SPEKE, SRP, ...*

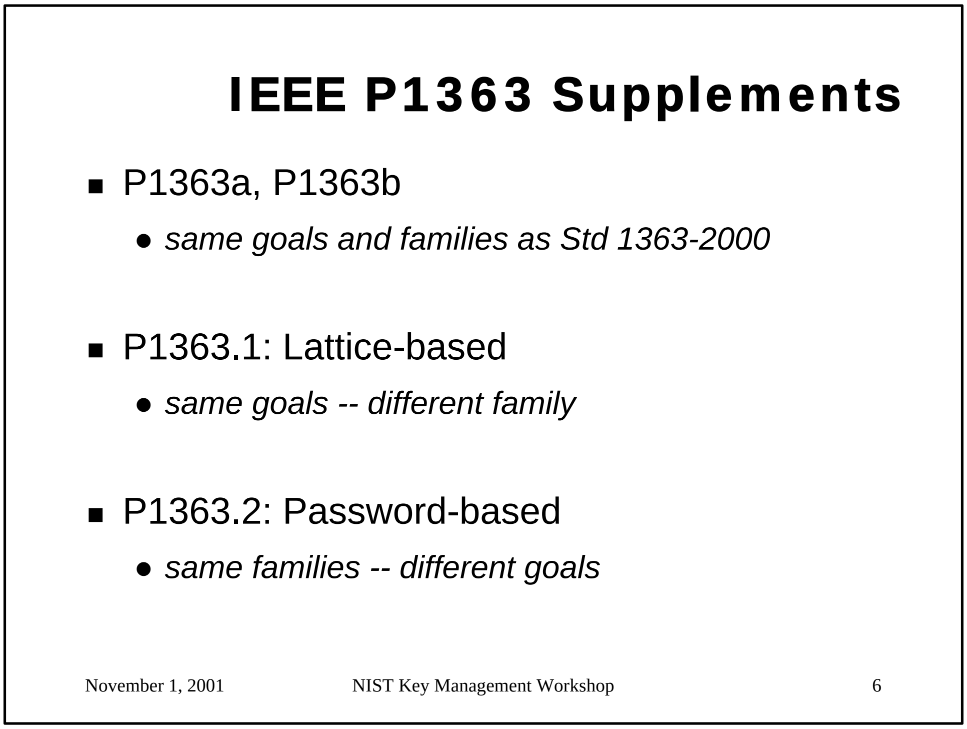
November 1, 2001 NIST Key Management Workshop 4



## History of P1363.2

- Password-based submissions to P1363
  - *1996 through 2001*
- Work deferred to a P1363 supplement
  - *while Std 1363-2000 completed*
- P1363.2 PAR approved
  - *late 2000*
- Latest draft
  - *October 23, 2001*

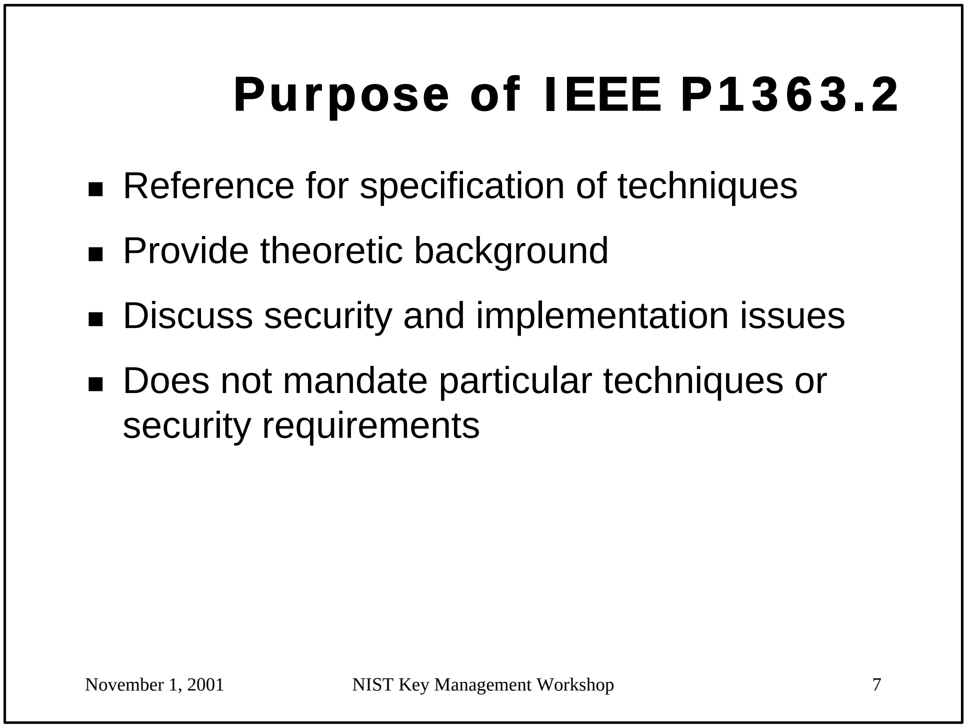
November 1, 2001 NIST Key Management Workshop 5



## IEEE P1363 Supplements

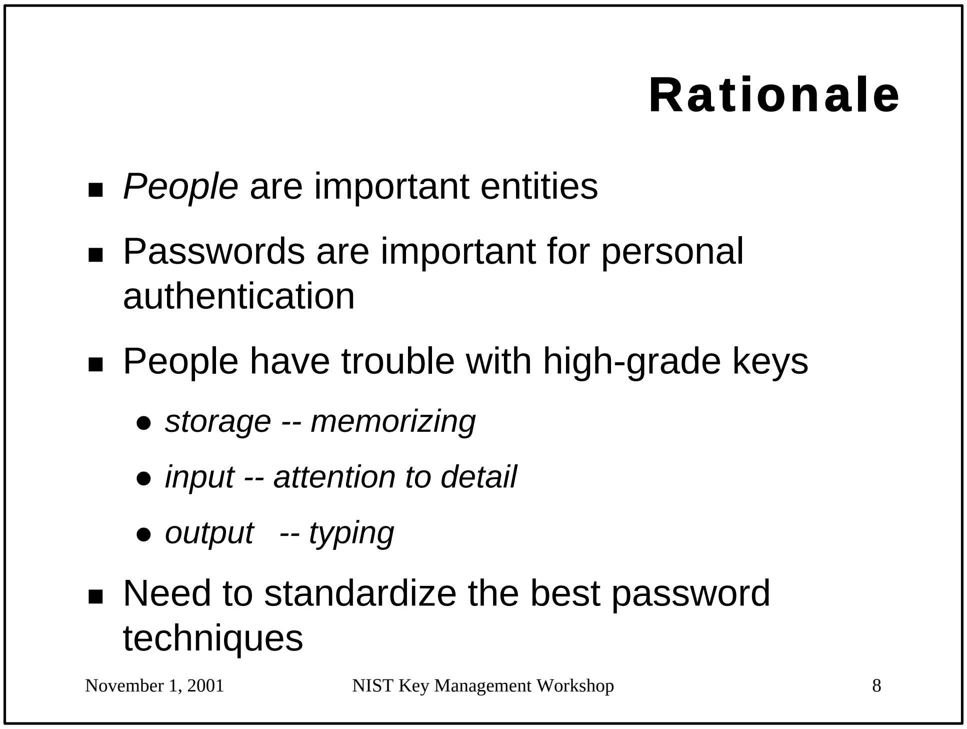
- P1363a, P1363b
  - *same goals and families as Std 1363-2000*
- P1363.1: Lattice-based
  - *same goals -- different family*
- P1363.2: Password-based
  - *same families -- different goals*

November 1, 2001 NIST Key Management Workshop 6



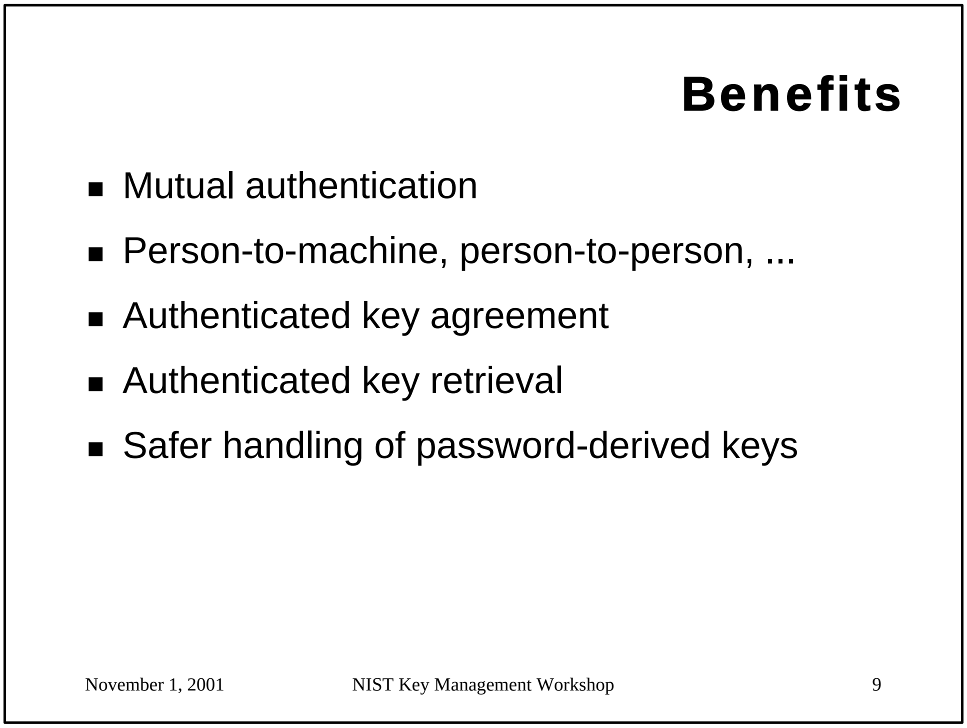
## Purpose of IEEE P1363.2

- Reference for specification of techniques
- Provide theoretic background
- Discuss security and implementation issues
- Does not mandate particular techniques or security requirements



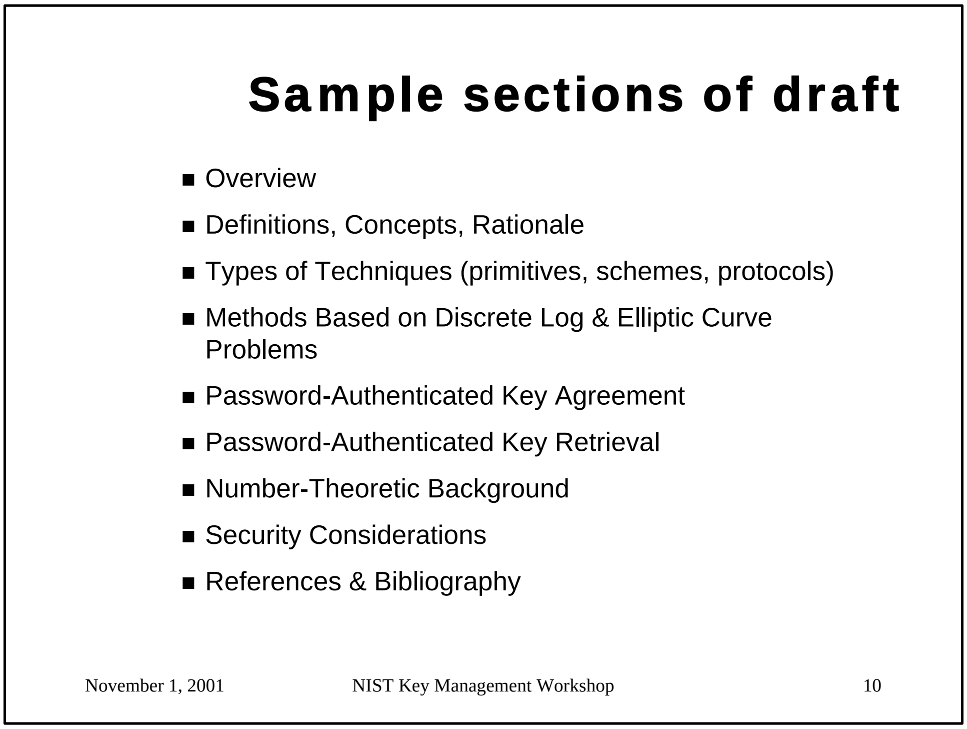
## Rationale

- *People* are important entities
- Passwords are important for personal authentication
- People have trouble with high-grade keys
  - *storage -- memorizing*
  - *input -- attention to detail*
  - *output -- typing*
- Need to standardize the best password techniques



## Benefits

- Mutual authentication
- Person-to-machine, person-to-person, ...
- Authenticated key agreement
- Authenticated key retrieval
- Safer handling of password-derived keys



## Sample sections of draft

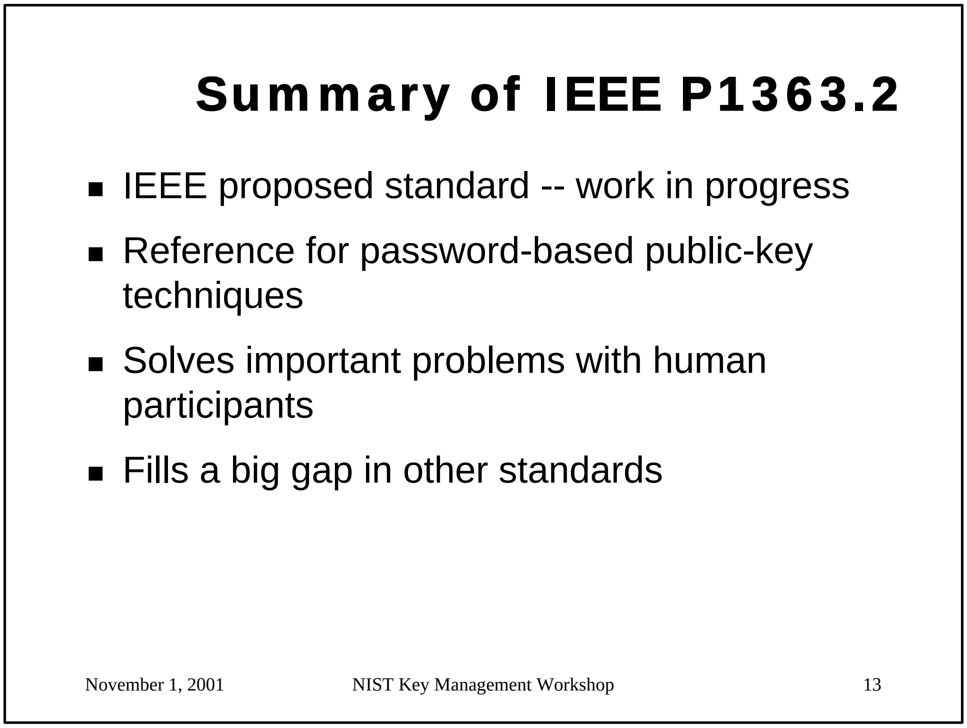
- Overview
- Definitions, Concepts, Rationale
- Types of Techniques (primitives, schemes, protocols)
- Methods Based on Discrete Log & Elliptic Curve Problems
- Password-Authenticated Key Agreement
- Password-Authenticated Key Retrieval
- Number-Theoretic Background
- Security Considerations
- References & Bibliography

## Example of a PKA Scheme

- *Password-authenticated Key Agreement Scheme (PKAS) operation for each party:*
  - Password ($p$) → ***PEPKGP*** →
    password-entangled public key (*w*)
  - Send *w* to other party
  - Get password-entangled public key (*w'*)
    from other party
  - $p$ ,*w'* ® ***SVDP*** ® agreed value *z*

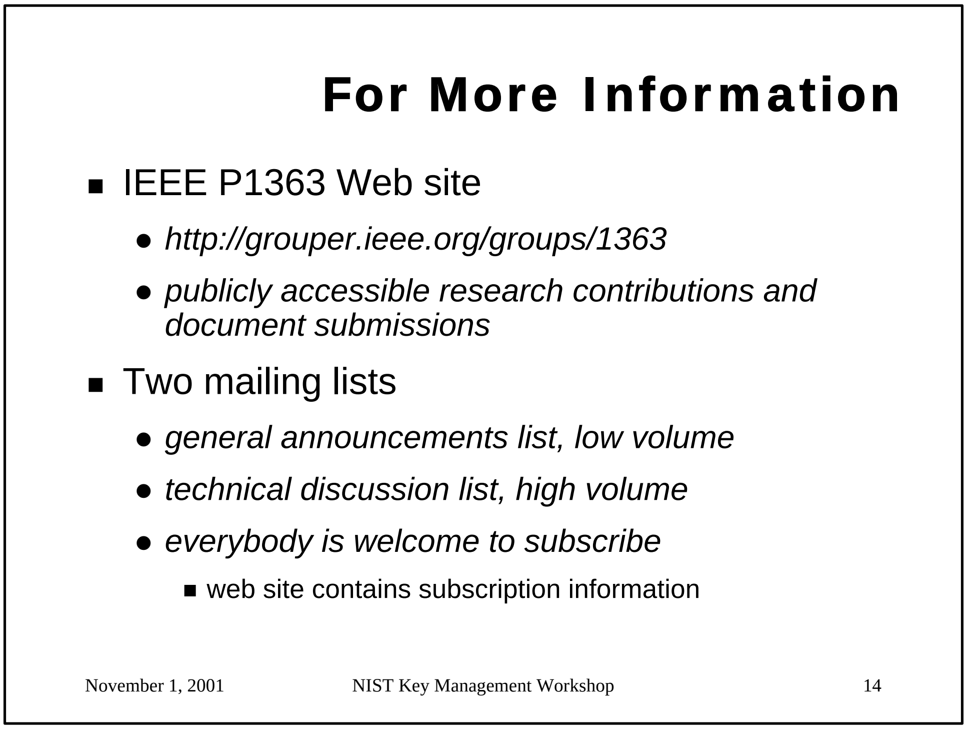
## Example of a PKA Primitive

- *Password-entangled Public Key Generation Primitive (PEPKGP) operation:*
  - Input:
    - $p_n$ *password-derived mask group element*
    - *s* *private key*
    - *g* *domain parameter*
  - Compute $w = (g\hat{}s) * p_n$
  - Output: *w*



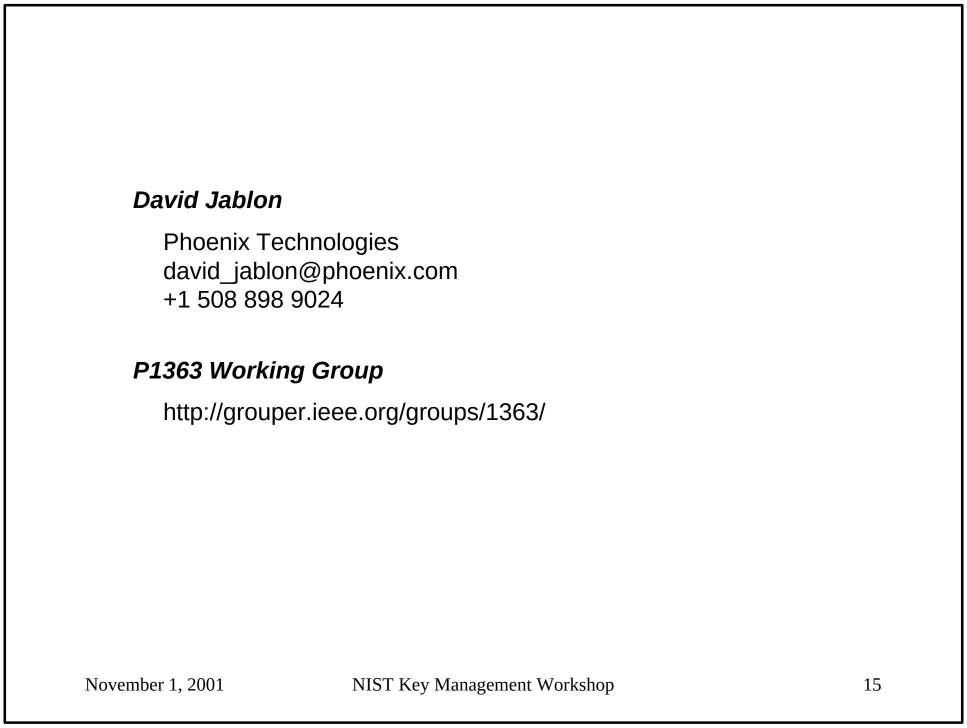
## Summary of IEEE P1363.2

- IEEE proposed standard -- work in progress
- Reference for password-based public-key techniques
- Solves important problems with human participants
- Fills a big gap in other standards



## For More Information

- IEEE P1363 Web site
  - *http://grouper.ieee.org/groups/1363*
  - *publicly accessible research contributions and document submissions*
- Two mailing lists
  - *general announcements list, low volume*
  - *technical discussion list, high volume*
  - *everybody is welcome to subscribe*
    - web site contains subscription information



***David Jablon***

Phoenix Technologies
david_jablon@phoenix.com
+1 508 898 9024

***P1363 Working Group***

http://grouper.ieee.org/groups/1363/