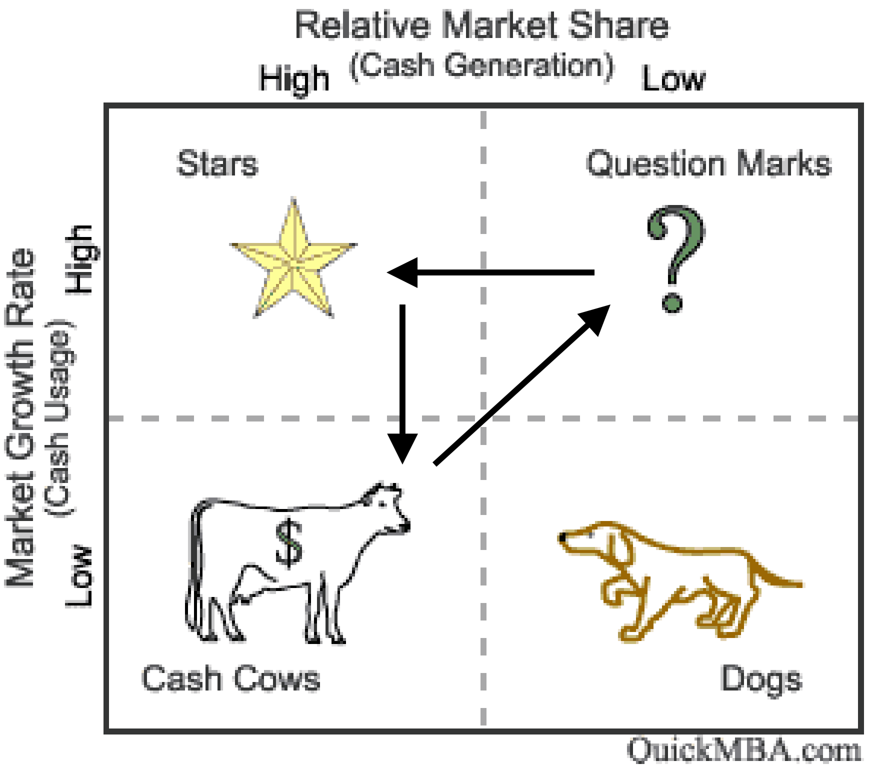
# Challenge & Response within E-Authentication Framework

NIST Symposium

February 9, 20004

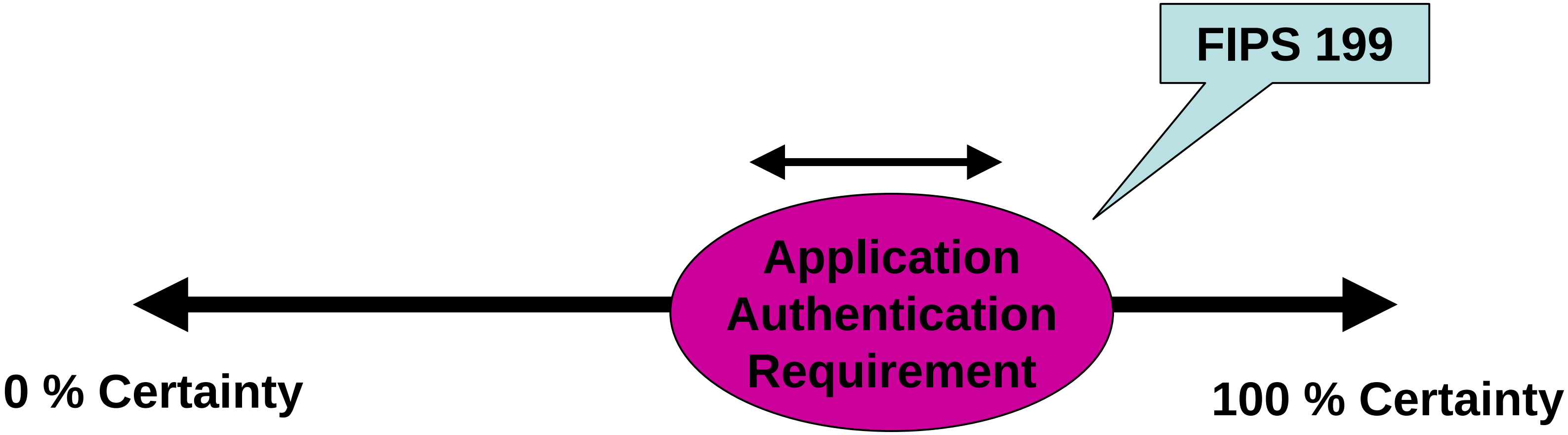
# The BCG Matrix: An Example of The Elegance of Simplicity



# E-Authentication Document Framework

| OMB E-Authentication Guidance<br>12/16/03 | NIST SP 800-60<br>Vol 1 & 2<br>FIPS 199 | NIST SP 800-63 |
|---|---|---|
| Sets framework for authentication levels 1 through 4 | Provides guidance for setting security and authentication level requirements for agency systems & applications | Provides guidance for technical implementation of e-authentication guidance |

# Identity Proofing Process



FIPS 199

Application Authentication Requirement

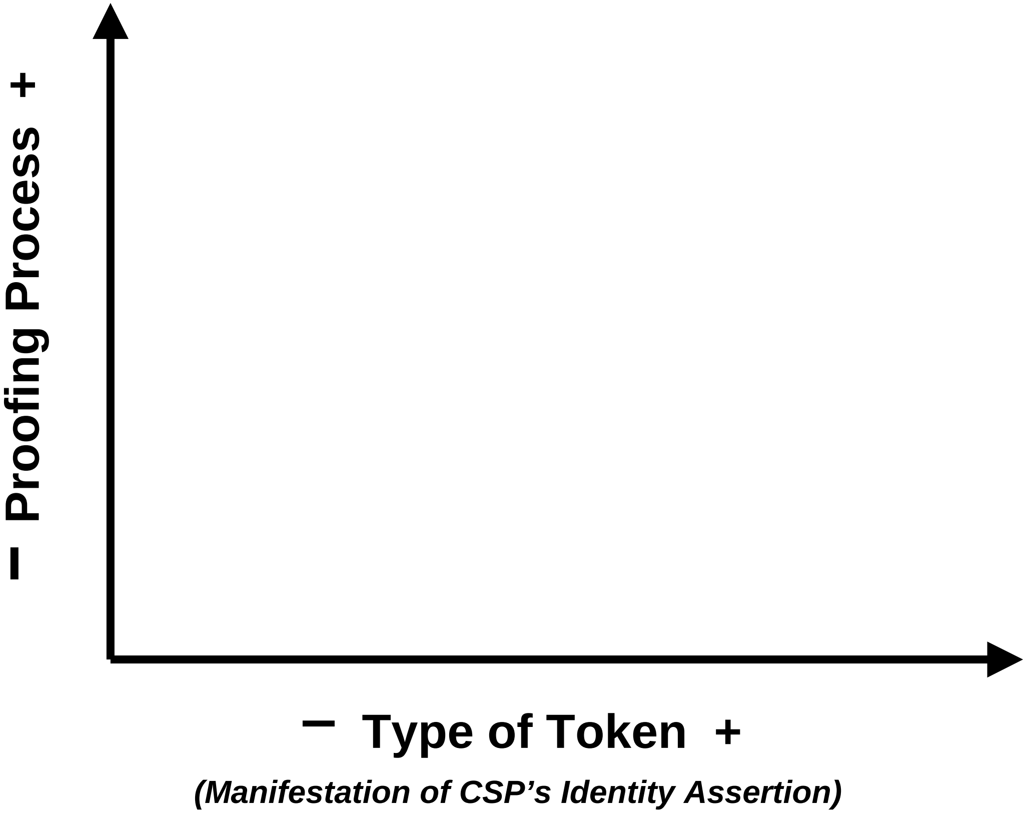
0 % Certainty

100 % Certainty

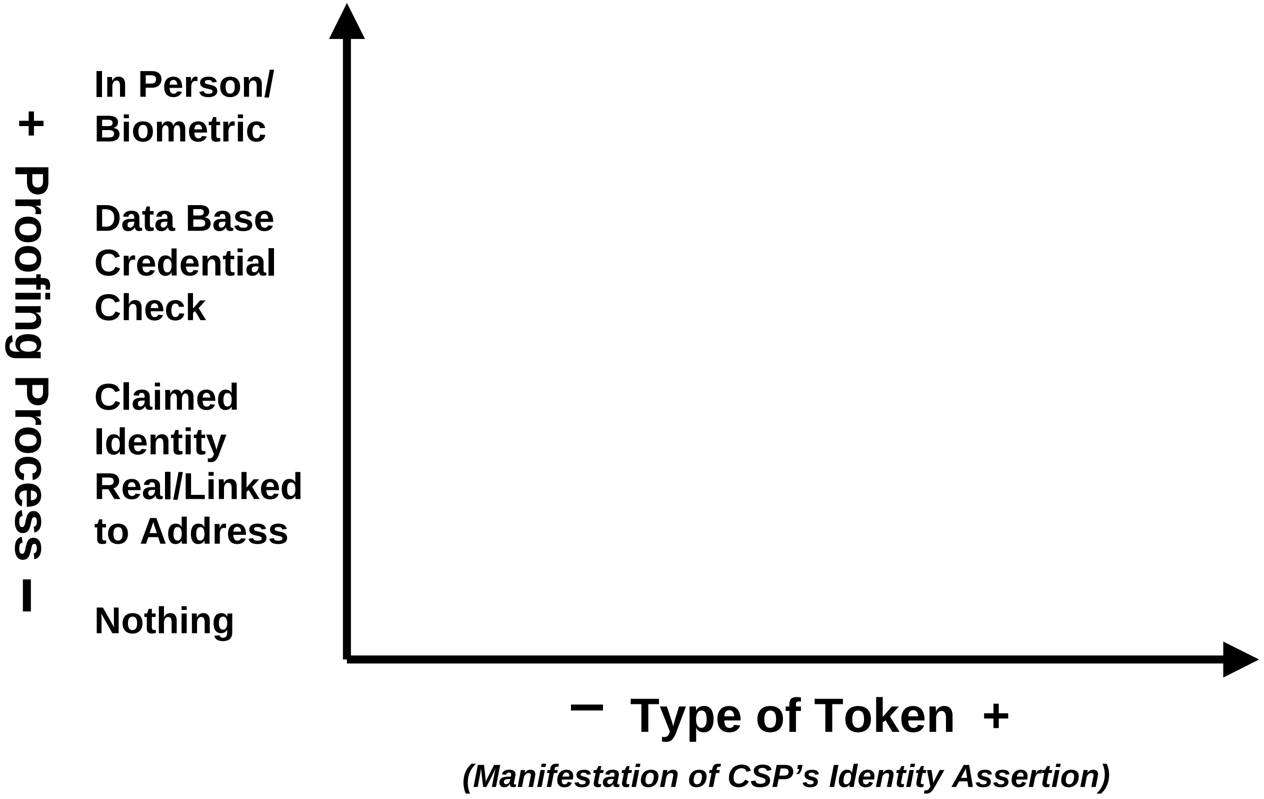
**Issues:**

- **Required Degree of Certainty**
- **Security of Authentication Protocol**
- **Time**
- **Cost**
- **Usability**

# E Authentication Framework



# E Authentication Framework



+ Proofing Process –

In Person/
Biometric

Data Base
Credential
Check

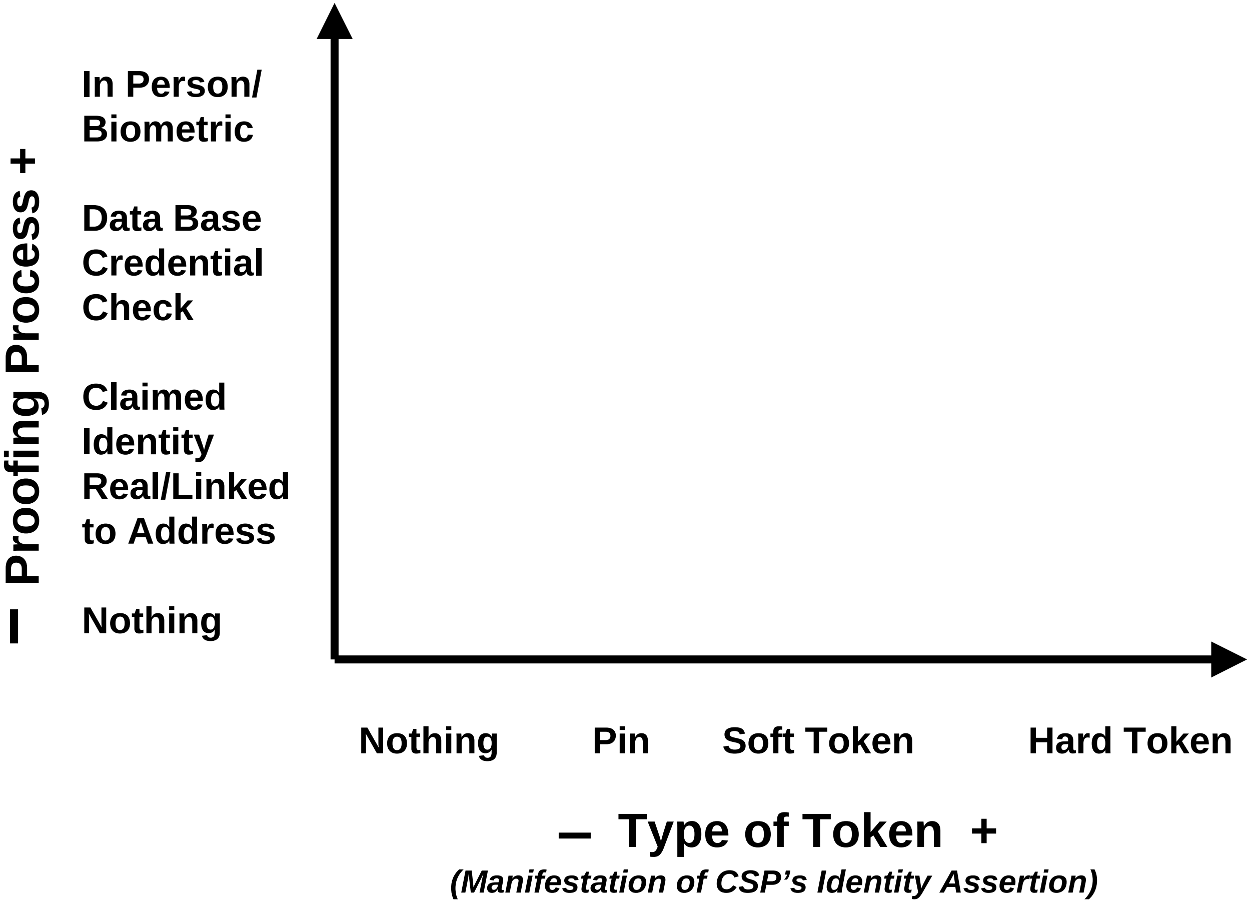
Claimed
Identity
Real/Linked
to Address

Nothing

– Type of Token +

***(Manifestation of CSP's Identity Assertion)***

# E Authentication Framework



– Proofing Process +

In Person/
Biometric

Data Base
Credential
Check

Claimed
Identity
Real/Linked
to Address

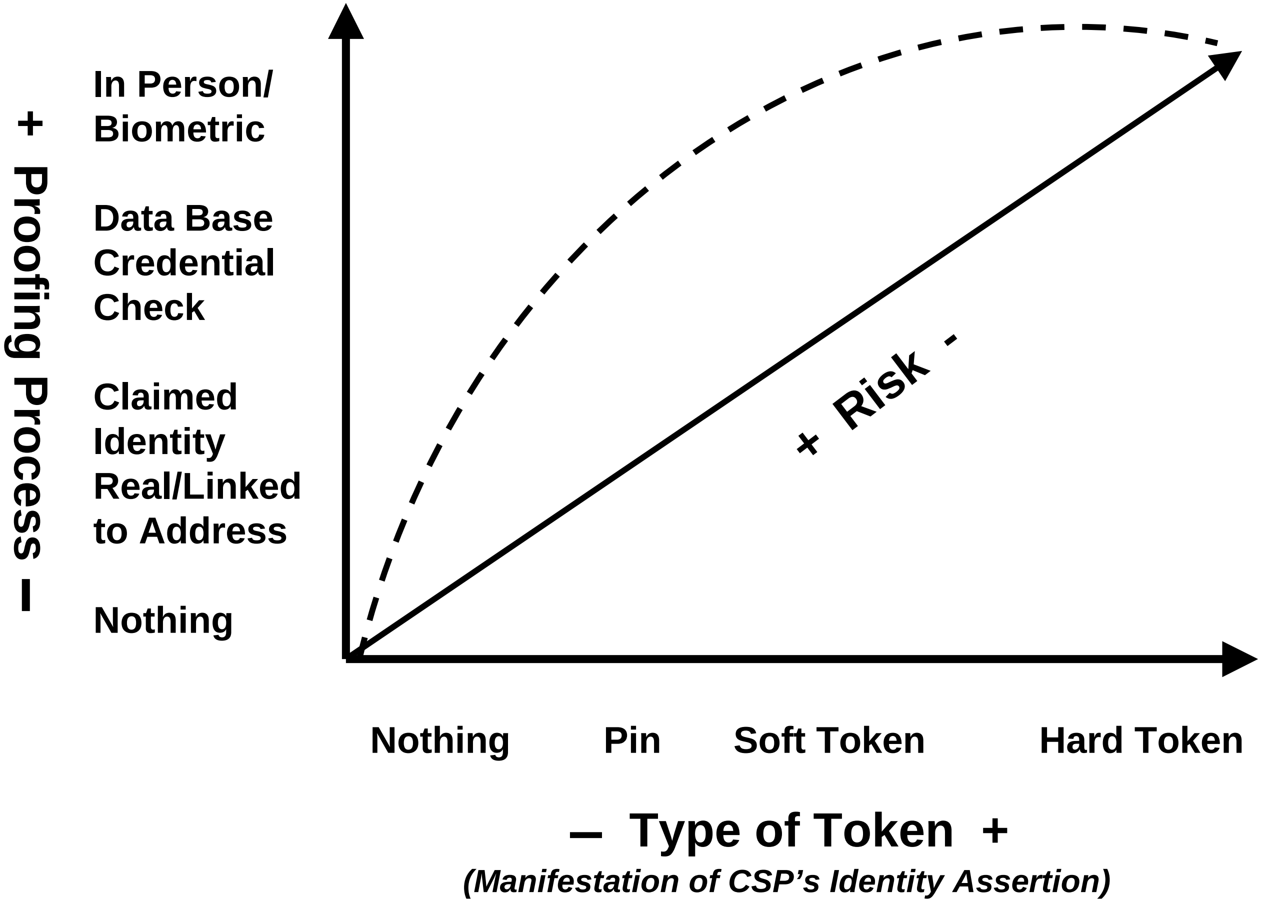
Nothing

Nothing Pin Soft Token Hard Token

**– Type of Token +**

***(Manifestation of CSP's Identity Assertion)***

# E Authentication Framework



+ Proofing Process –

In Person/
Biometric

Data Base
Credential
Check

Claimed
Identity
Real/Linked
to Address

Nothing

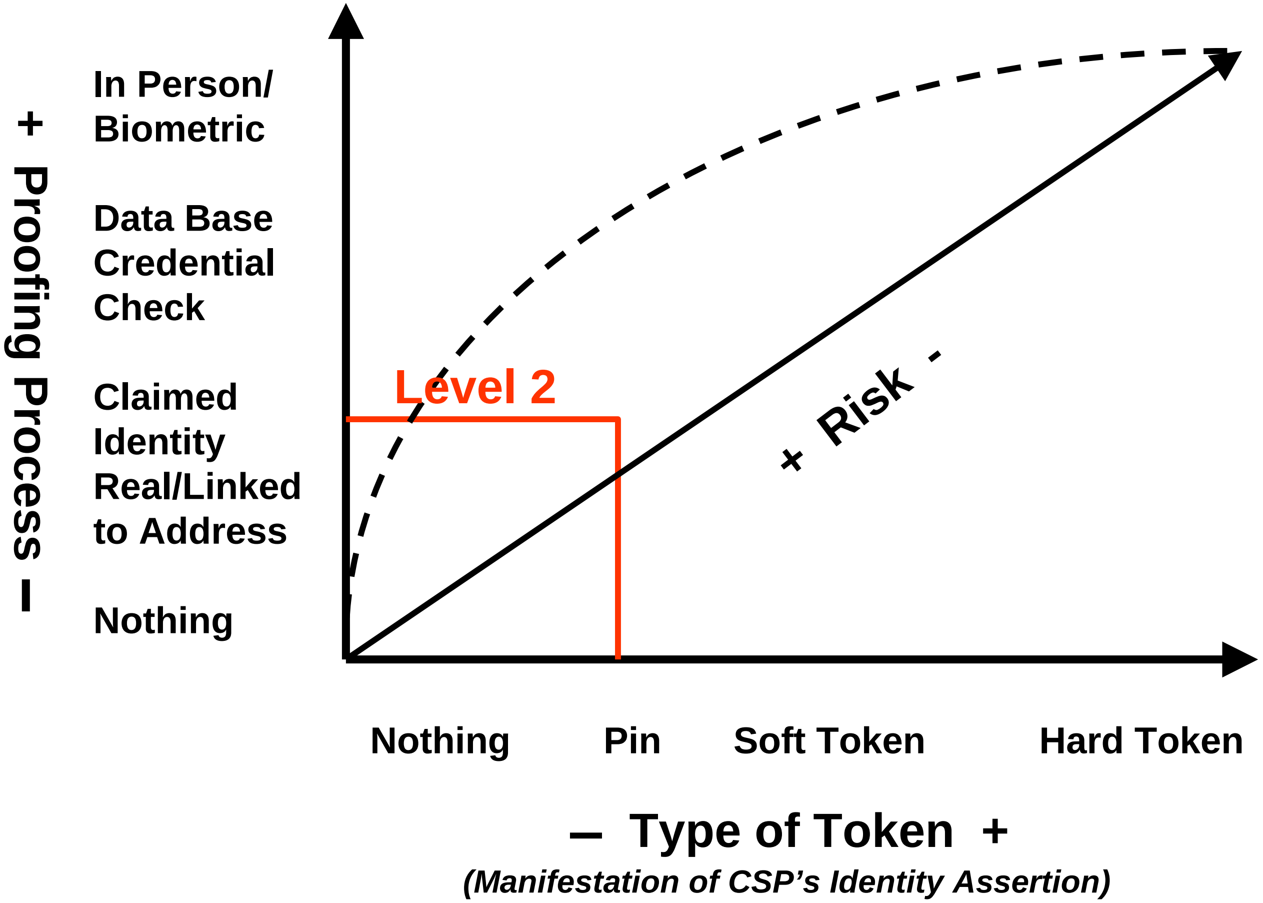
+ Risk -

Nothing Pin Soft Token Hard Token

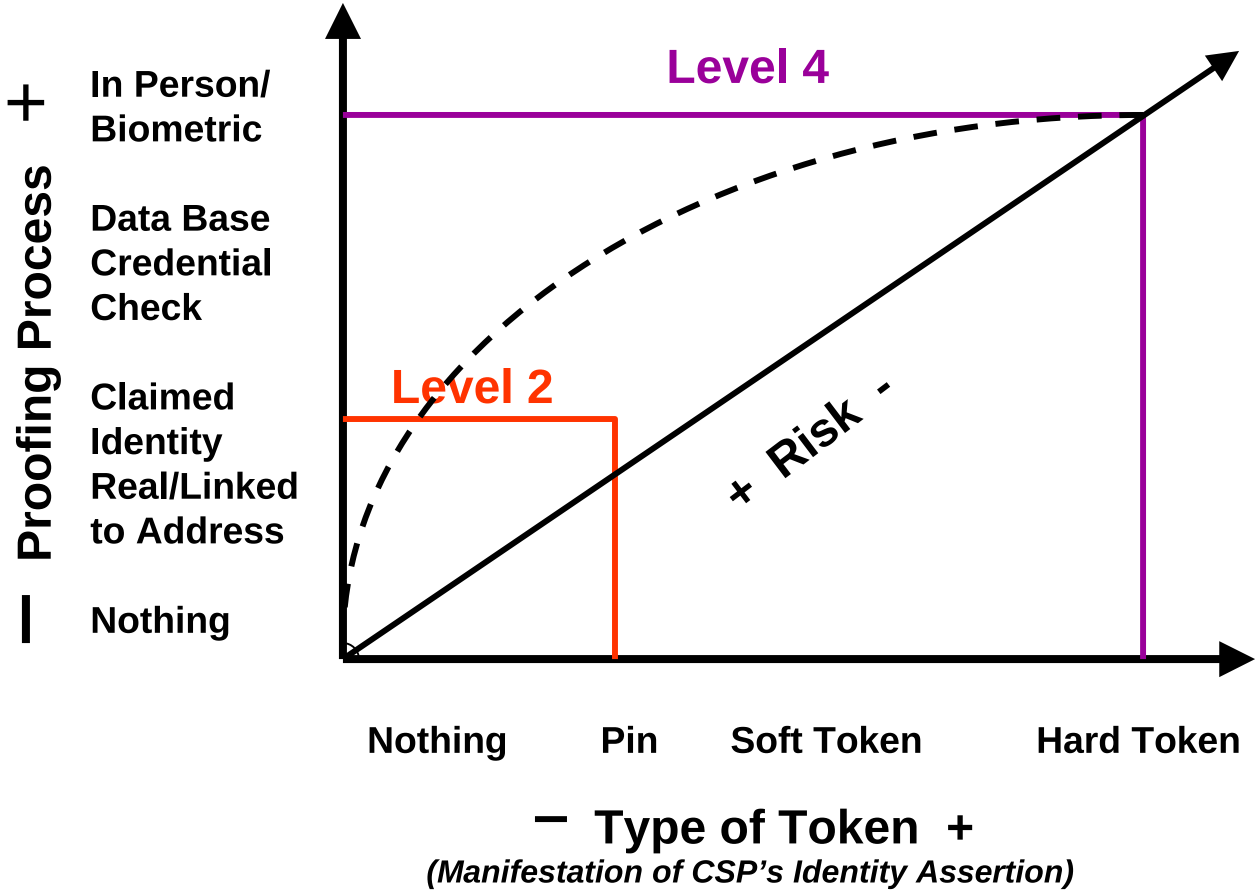
– Type of Token +

*(Manifestation of CSP's Identity Assertion)*

# E Authentication Framework



# E Authentication Framework



# Issues Surrounding Information Used in Identity Proofing

- Types of Information
- Characteristics of Information
- Availability/Visibility of Information
- Sources of Information
- Percent Coverage
- Cost of Information

# Types of Information

- Family
- Physical
- Education Background
- Financial
- Employment
- Health
- Psycho-graphic

# Characteristics of Information

- Static Information
  - Place of Birth
  - Date of Birth
  - Education
  - Blood Type
  - Military Service
  - Mother’s Maiden Name

- Dynamic Information
  - Marital Status
  - Employer
  - Job Title
  - Address
  - Telephone Number

# Availability of Information

- General Availability
- Degree of Aggregation
- Discoverability
- Privacy Constraints
- Accuracy

# Cost of Information

- Aggregators Supply Raw Material to Most Authentication Schemes
- Aggregators will be Low Cost Producers and Set Pricing Models for Industry

# Challenge Response Issues

- Types of Questions
- How Many Questions
- Range of Tolerances
- Benefits of Time Limits
- Need for Archiving

# Types of Questions

- Mix of Static and Dynamic Facts
- Claimant May Not Have to Know the Answers
- At the End of the Day, All Answers Probably Discoverable
- Security Comes from Randomness

# How Many Questions

- Ying and Yang of Security vs. Usability
- 3 to 5 Questions Probably Max if User to be Willing Participate

# Range of Tolerances

- Wrong May not  be All Bad
- Ill Prepared Claimant May be Reasonably within the Ballpark
- Case Can be Made for Well Prepared Attacker Getting All Right

# Benefits of Archiving Results

- Avoids Duplication and/or Learning
- Cost/Benefit Analysis Needed
- May be Security Requirement

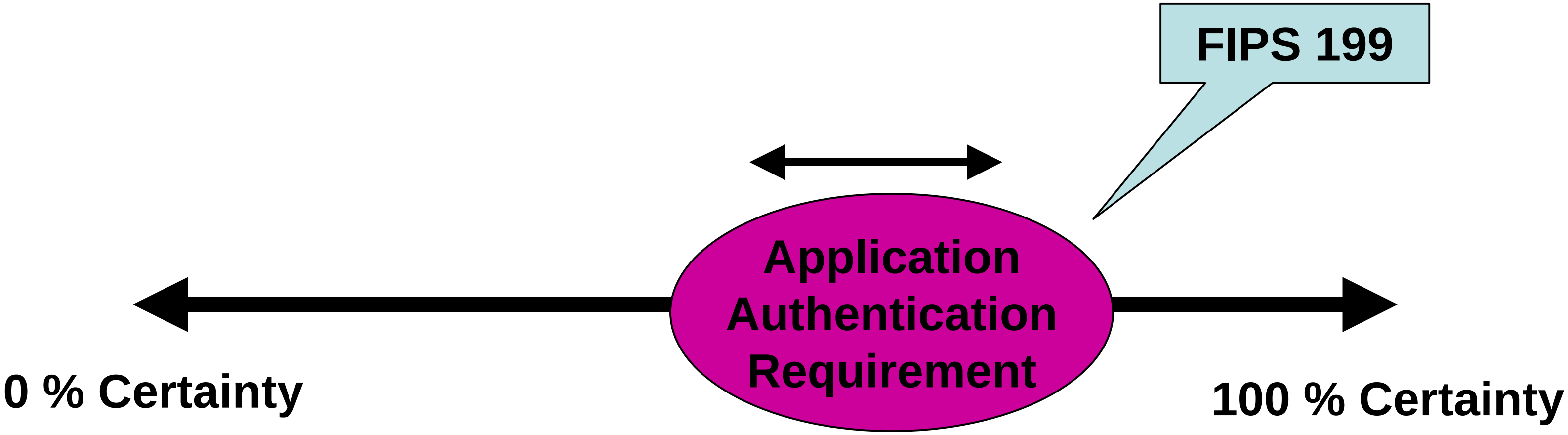
# Scoring Issues

- Probalistic Models
- Often Geared to Organizations “Unique” Customer Base
- Require Large Number of Historical Transactions
- Base Upon Acceptance of: “You Can’t Get it All Right, All the Time.”

# E-Authentication Document Framework

| OMB E-Authentication Guidance<br>12/16/03 | NIST SP 800-60<br>Vol 1 & 2<br>FIPS 199 | NIST SP 800-63 |
|---|---|---|
| Sets framework for authentication levels 1 through 4 | Provides guidance for setting security and authentication level requirements for agency systems & applications | Provides guidance for technical implementation of e-authentication guidance |

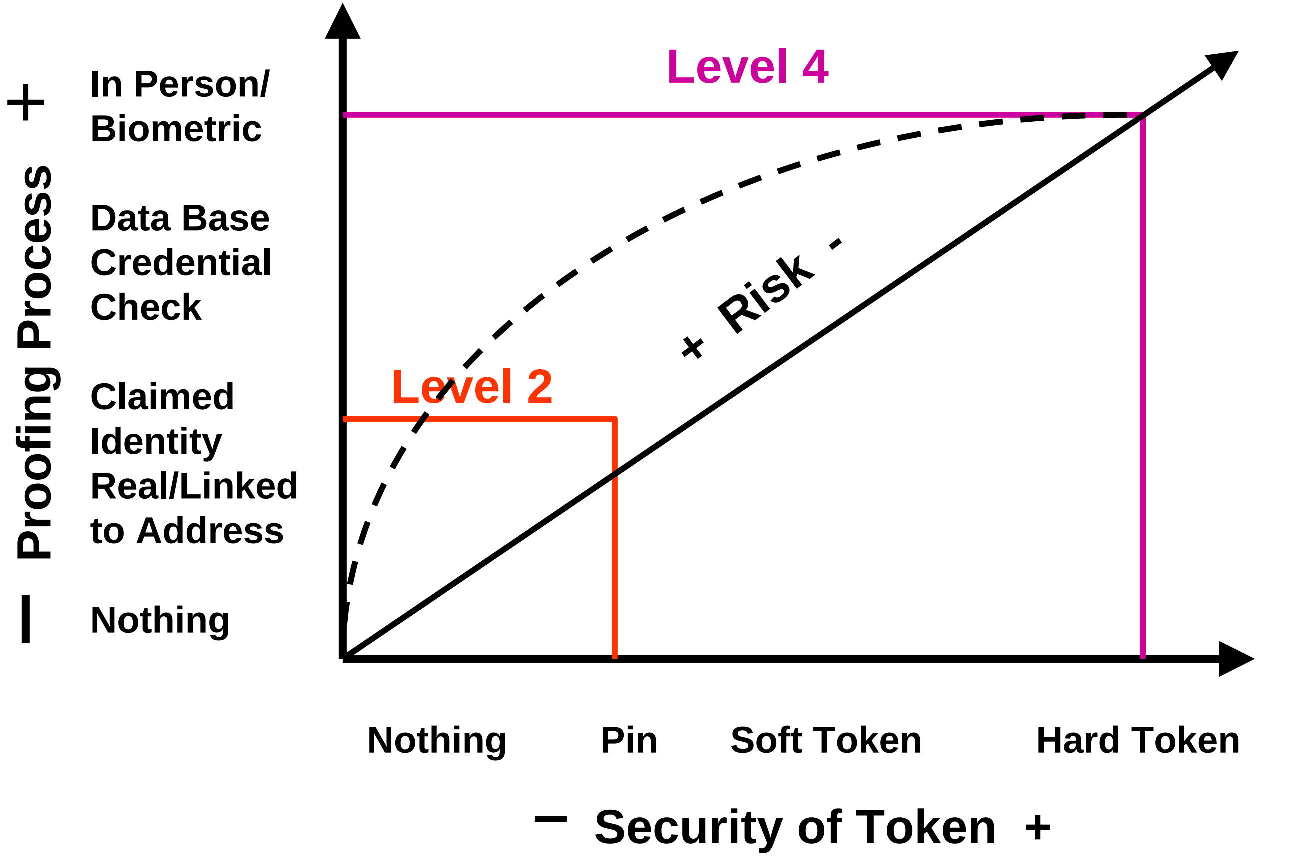
# Identity Proofing Process



**Issues:**

- **Required Degree of Certainty**
- **Security of Authentication Protocol**
- **Time**
- **Cost**

# E Authentication Framework



Level 4

Level 2

+ Risk -

+ Proofing Process –

In Person/ Biometric

Data Base Credential Check

Claimed Identity Real/Linked to Address

Nothing

Nothing

Pin

Soft Token

Hard Token

– Security of Token +

***(Manifestation of CSP's Identity Assertion)***

# For Additional Information, Arguments, or Debates

Scott Lowry

President, Diversinet USA

scott@diversinet.com

202.236.8221