



Identify yourself securely.™

True Identity™ solution

True Identity authentication and authorization for groundbreaking security across multiple applications including all online transactions

Biogy Inc. Copyright © 2013

A major crisis exists with the current state of cybersecurity technology.

Even the largest institutions cannot be protected from cyberattacks.

<http://www.foxbusiness.com/industries/2012/10/05/version-bank-cyber-attack-tools-found-in-saudi-arabia/>

The authorization of an action by users is not securely bound to the identity of an individual.

A digital identity (e.g., SSN or cryptography key) is a virtual identity; it is not a true identity of a living person.

Weaknesses of security systems offered by security providers

- **Untrusted Browser attacks.** Transaction authorization can be circumvented after strong authentication.
<http://www.technologyreview.com/computing/23488/?a=f>
No solution exists. Financial transactions can't be adequately protected.
- **Centralization.** Seeds, which are used to create each one-time passcode, are generated and centrally stored.
- **Digital Identity.** A digital identity can be reproduced, transferred, or stolen.

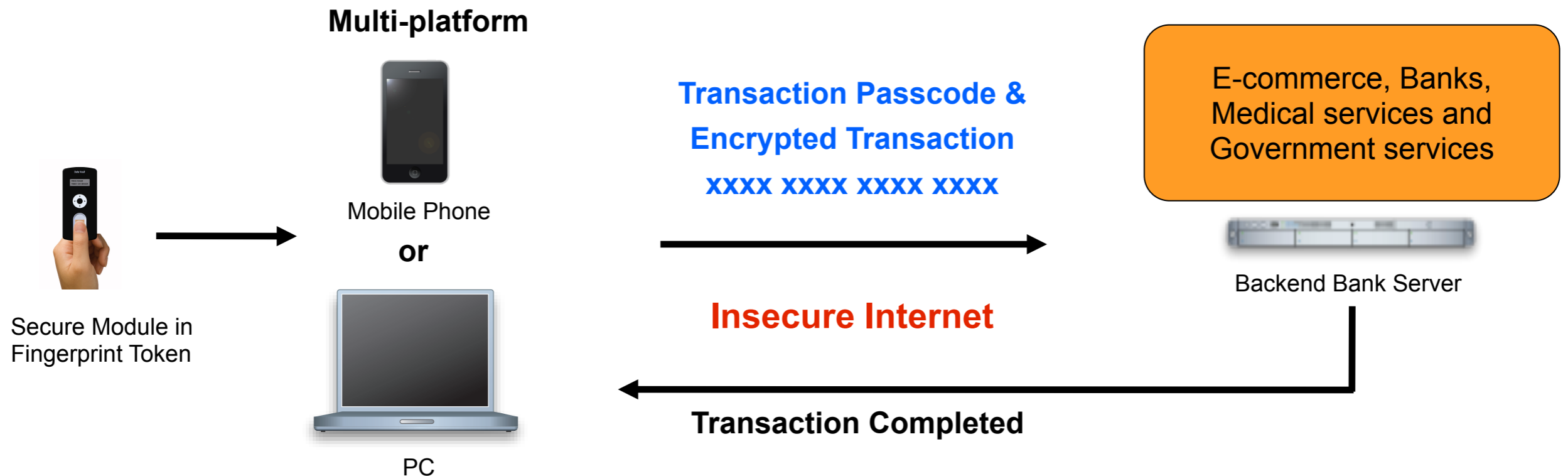
Weaknesses of security systems offered by security providers II

- **Shared secret.** The backend and device use a shared secret. A backend break-in compromises the shared secret on the token devices.
- **Determinism.** Seeds and one-time passcodes are created by deterministic algorithms, calculated from a **secret seed, serial number** unique to that token device and the **time of day**. **Reverse engineered algorithms, secret seed, serial number and phished PIN breaches the system.**



Only Biogy technology offers a solution that overcomes inherent limitations of current security technology. *True Identity™* is the answer to next generation computer and network security.

Biometric *True Identity*TM sends an unpredictable malware resistant **Transaction Passcode**



Biometrics and personal identification information exist only in secure module. Personal data and biometrics are never transmitted over insecure lines.



True Identity Use Case Steps

Step 1. User presses appropriate finger on sensor of Biogy token.

Step 2. A valid fingerprint match generates a one-time transaction passcode.

Step 3. Transaction passcode and encrypted transaction information is transmitted to bank backend server via mobile phone, PC or other.

Step 4. Backend bank server verifies transaction passcode and transaction information. If valid, do step 5a. If invalid, do step 5b.

Step 5a. Transaction is executed. Confirmation notification.

Step 5b. Transaction is aborted.



Groundbreaking Security Solution

- **Asymmetry.** Backend breaches don't compromise the devices.
- **Decentralization.** Passcode generators are created on the token device. *The system can only be hacked one hardware device at a time.* Seeds cannot be stolen from the network because they do not exist on the network.
- **Dynamic.** Unlike seeds, passcode generators change over time.
- **Stops untrusted browser attacks.** Malware can't steal what it can't understand. NMP malware resistant technology is integrated with the Biogy fingerprint-protected token.

- **True Identity.** A valid, local, biometric authentication is securely linked to cryptographic operations. All confidentiality, integrity and authentication and transaction operations are executed in a secure embedded environment. *True Identity™* cannot be stolen.
- **Non-Determinism.** The solution does not require pseudo-random number algorithms to create unpredictability. Reverse engineering of algorithms does not reveal any critical information. Over 100,000 bits of true entropy are created during enrollment.