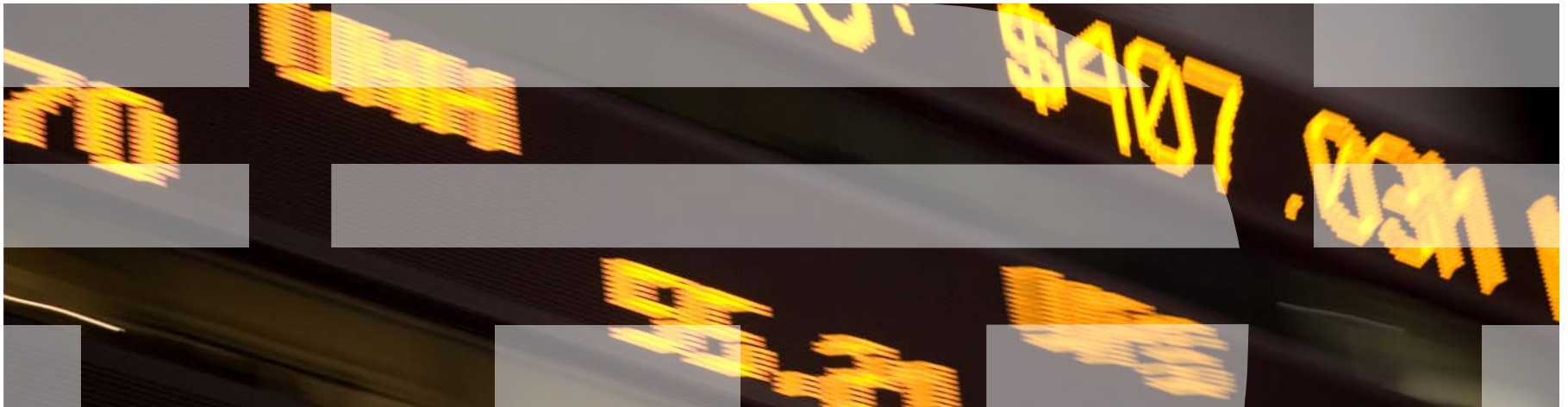


Smart e-banking: Neue Lösung aus der IBM Forschung IBM Zone Trusted Information Channel ("ZTIC")



IBM Research – An Overview (Security Aspects)



BlueZ Business Computing

- We're part of the Computer Science department of ZRL working on
 - Cryptographic/PKI Libraries - used in many IBM products
 - First-time (IBM) implementations as well as standardization work
 - Definition and Development of open, standard chip card security software
 - Embedded software & development software (e.g., Eclipse Tooling)
 - Standardization work, e.g., ISO18013 (chipped driver's licenses)
 - Direct customer engagements
 - particularly in the banking and government industry
 - ODIS: Work in consulting engagements on "hard" problems (e.g., performance, longevity of signatures, ease-of-use)



Authentication: Threat-Solution Taxonomy

Where are we today?

➤ MELANI report (11/07):

“Two-factor authentication systems (e.g. transaction authentication numbers, SecurID, etc.) do not afford protection against such attacks and must be viewed as insecure once the computer of the customer has been infected with malware.

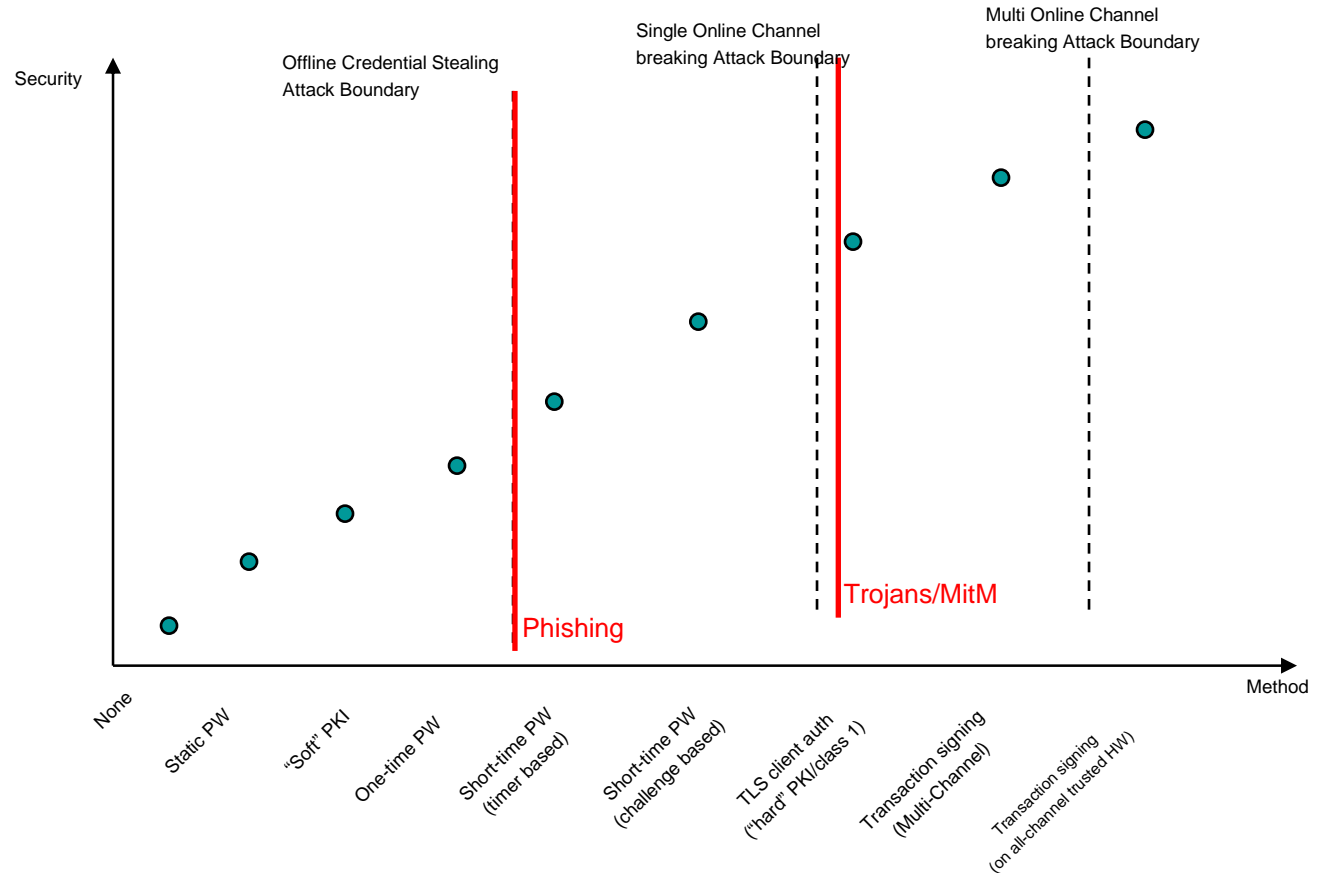
[...]

Websites installing malware on the computer without any action by the user (*drive-by infections*) have heavily increased as an infection vector.”

(Swiss Federal Police)

➤ Symantec (01/08)

Trojan.Silentbanker targets 400 banks and changes transaction details “silently” – even in the presence of two-factor authentication



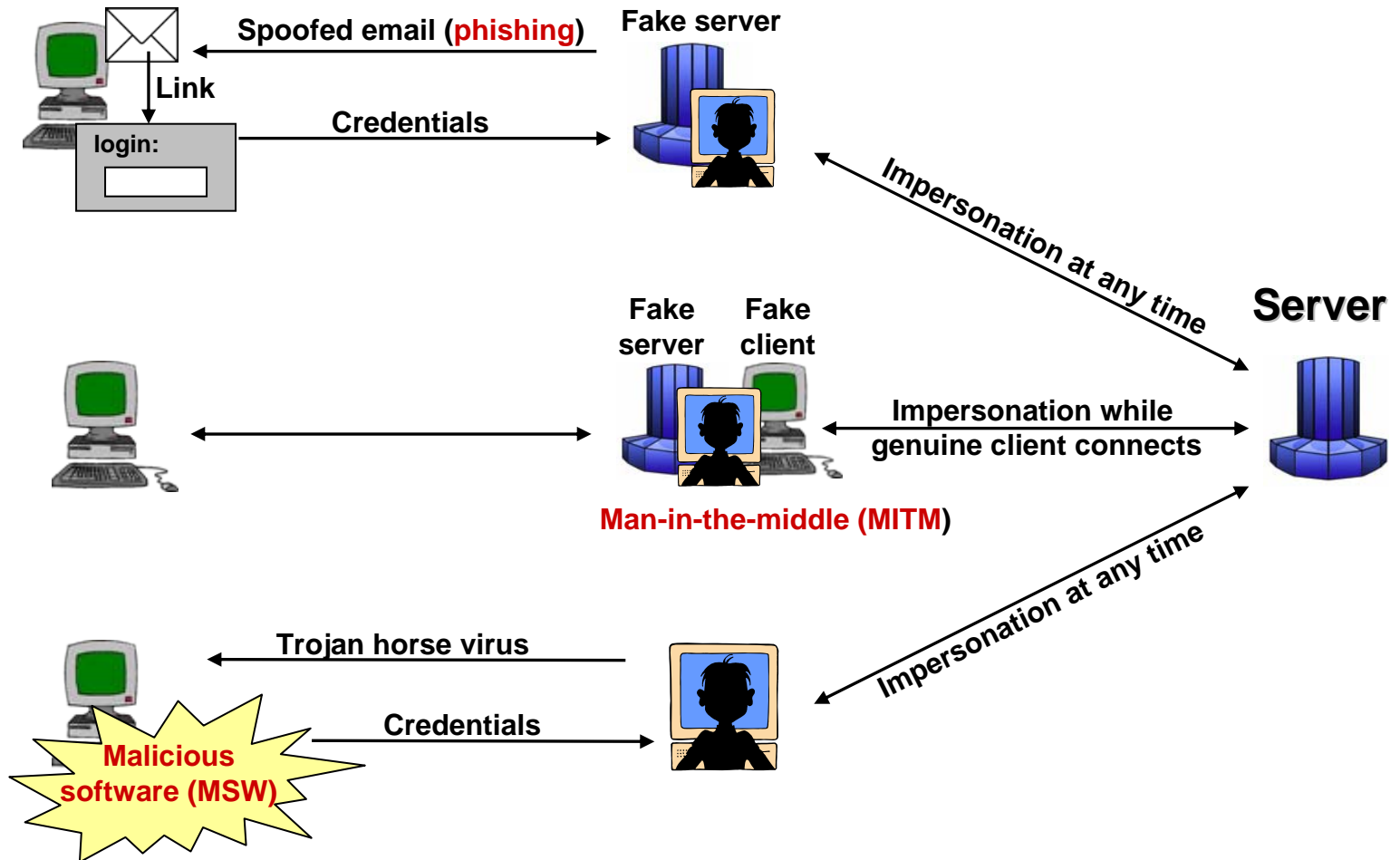
What is the problem?

- User PCs are under attack
 - Attack vectors (selection)
 - Spam (mail): “Click-and-be-doomed”
 - Some “free helper tools”
 - “popular” websites (porn, warez, etc.): “Drive-by infection”
 - Google-found websites
 - Sample attack method (beyond traditional vulnerability and standard API exploits)
 - APEG (Automatic Patch-based exploit generation)
 - Attack goals (selection)
 - Turn the computer into a zombie (for a botnet) or “kidnap” data (for ransom)
 - Obtain login-IDs/PINs (e.g., using key-loggers)
 - Re-route transaction information (e.g., using display-changers)
 - Attack professionalism
 - Very high and rising (task “outsourcing”, physical “enforcement” becoming the norm)
 - To some accounts, e-crime is already more profitable than drug trafficking

How serious is the problem?

- Size of the problem (Secunia Research)
 - At least 1/3 of all PCs are not properly patched
 - Only 1 security suite detects 20 % of exploits; the rest detects less than 4 %
- Completely “professional” industry doing malware (ISS Research)
 - EUR 250 for malware (p2p features cost EUR 50 more); 30 % deduction for known customers
 - “COTS” prices: €70 (screen grabber), €70 (password grabber), €300 (loader/distributor), ...
 - GBP 100 for weaponized exploit toolkit for 15 known program weaknesses
 - Trojan2Worm creation kits; online virus scan “protection” validator (incl. 4 month “warranty” against AV detection for specific malware); anti-debugging tools for malware creators; ...
- WW \$1.7bn of online banking customers’ money “accessible” to hackers (Symantec Research)
- >25’000 credentials stolen by one botnet (Torpig/Sinowal) alone per day (RSA Research)
- \$351 per US victim lost to phishing in 2008 alone: At 5M victims, that’s \$1.75bn (Gartner)
- So what?
 - For valuable transactions, you cannot trust what you type or see on your PC
 - Courts start to acknowledge this (e.g., in Germany) putting responsibility to combat online banking fraud onto banks

Authentication: Main Attack classes



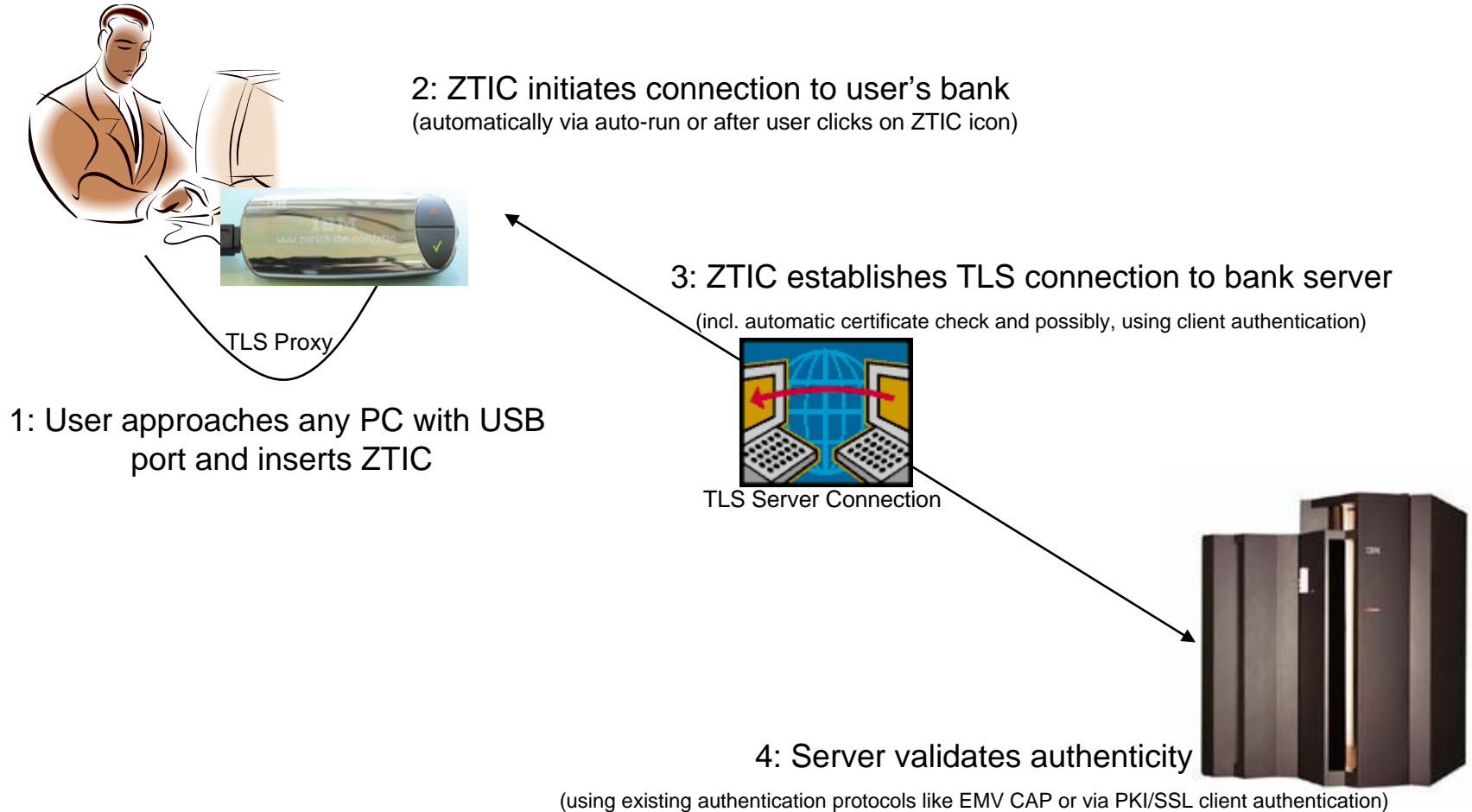
“ZTIC” Design Goals

- Protect against Malicious Software & Man-in-the-Middle Attacks
 - Do not rely on PC for input or output of critical data
- Do not require the installation of additional software
 - No special web browser (retain user experience, no need to re-train)
 - No device drivers (no new user/support center hassles)
- Be easy-to-use
 - Ease the transaction experience of present solutions
 - Use “familiar” device/interaction pattern
- Be easy-to-administrate & integrate
 - Do not require server changes
 - Re-use existing authentication protocols, e.g., CAP, PKI/SSL client-authentication
 - Allow for “fool-proof” device maintenance
 - Do not require additional customer support staff (due to special browsers, etc.)
- Be cost effective: At par with standard hardware dongles

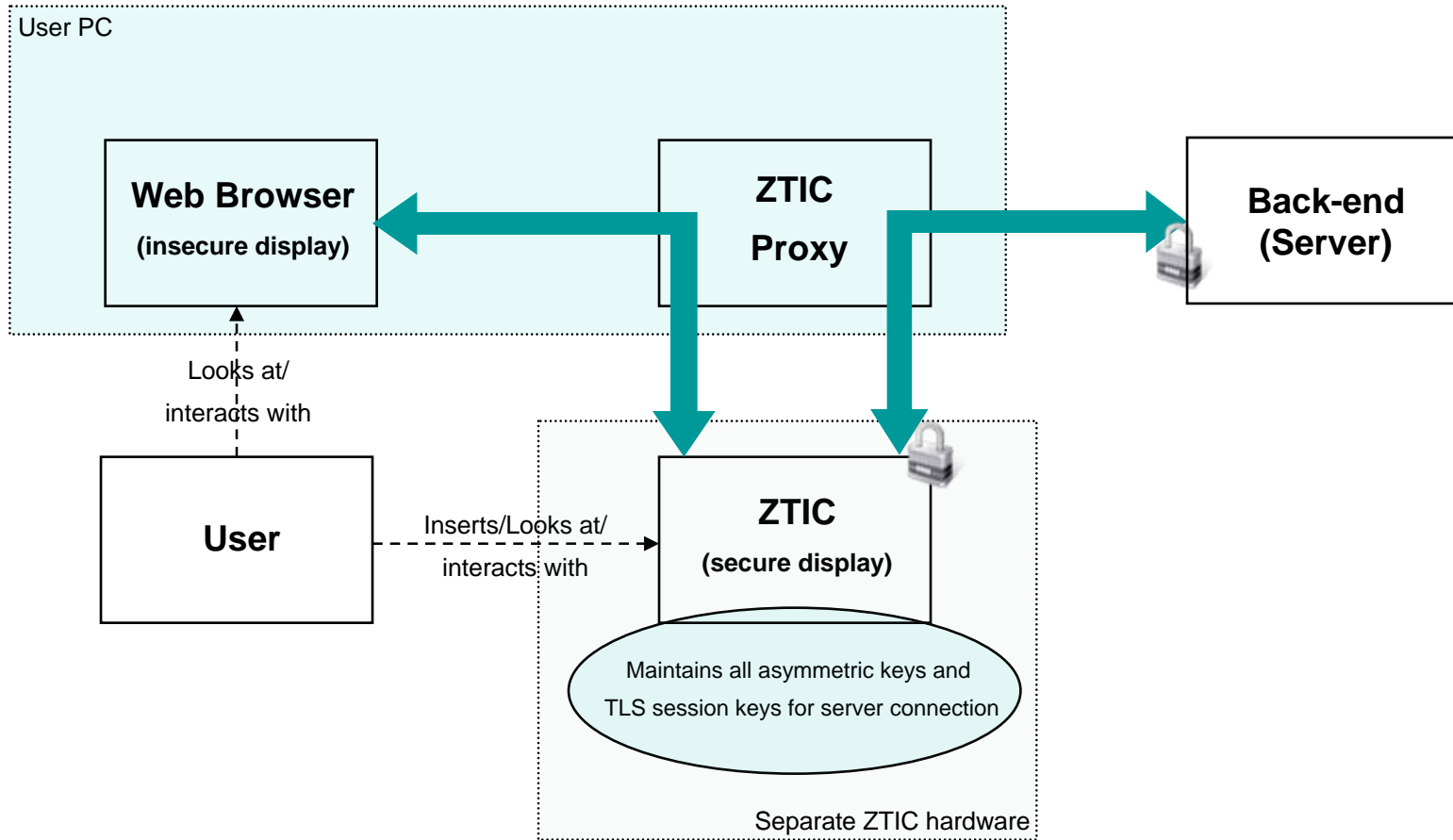
“ZTIC” Concept

- A USB Token with display and a button...
 - ... running SSL
 - Utilizing standard PKI (SSL server- & possibly, -client authentication) without server changes
 - Personalized for specific servers (only the “right” server can be contacted)
 - ... “reviewing” HTTP traffic that is to be protected
 - Showing actual transactions on the display
 - Requesting explicit user consent on sensitive operations
 - ... utilizing the file system USB protocol (“MSD”)
 - Works in all types of PCs (incl. Mac & Linux)
 - Does not require any software installation (“Insert-to-bank”)
- Options:
 - Using a smart card (ID0 or ID1) as a secure data container
 - Retaining existing production environments / authentication solutions
 - Remote configuration
 - Adaptation to server-specific profiles

“ZTIC”: How it works (high-level)



ZTIC™: How it works (In-Stream)



“ZTIC”: Behind the scenes (In-Stream)

- The web browser requests a Web page ...
 - ... via “localhost” using http(s to avoid caching)...
- ... the ZTIC decrypts data received from the server via the “localhost” proxy
- ... the proxy re-writes all links on the page and marks authentication elements
- Upon transmission of a specific authentication operation, the ZTIC internally ...
 - ... fills in known data (account information, passwords)
 - ... computes authentication responses
 - ... encrypts the response for transmission to the server
 - → Key data can be hidden completely from the web browser
- Upon submission of a “critical transaction” page, the ZTIC locally....
 - ... displays the transaction data
 - ... waits for the user to approve it
 - ... encrypts the transaction for transmission to the server
- As a result...
 - ... no security-sensitive data is kept on the PC
 - ... any tampered software on the PC (incl. proxy) will only cause the ZTIC to stop operating
 - → Appropriately educated users can stop and get their PC fixed



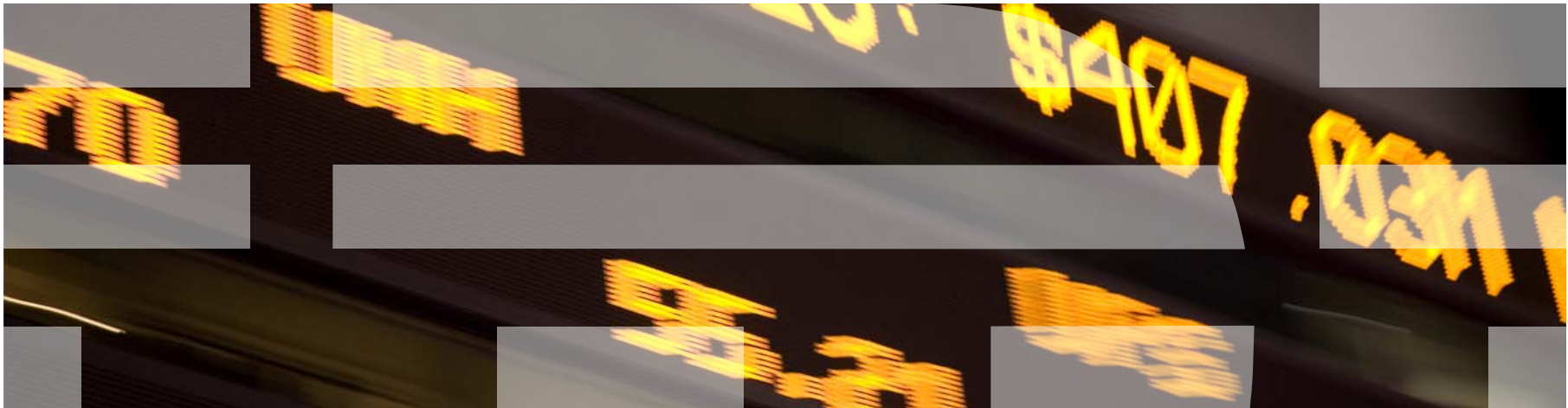
“ZTIC”: Core Advantages

- Security
 - Authentication, Integrity, Confidentiality → Operation of SSL/TLS (outside of PC)
 - Protection from
 - Malicious Software Attacks → Display of Critical Information (outside of PC)
 - Man-in-the-Middle Attacks → Mutually authenticated SSL/TLS channel (verified outside PC)
 - Phishing Attacks → Automatic session establishment with securely stored credentials (outside of PC)
 - → Always giving the user the “final say” (button press)
 - Non-Repudiation → Use of Smart Card and PIN
- User Convenience
 - Small Form Factor (→ key fob); well-known device type (→ MP3 player)
 - No requirement for (PC-)driver software installation (→ USB Mass Storage/memory stick)
 - Works on all PC types (→ tested on different Windows and Mac versions) incl. Win autorun
- Service-provider efficiency
 - Minimal (if any) server changes
 - Minimal (if any) customer support requirements
- Cost-efficiency: Standard hardware components used

“ZTIC”: Additional Advantages

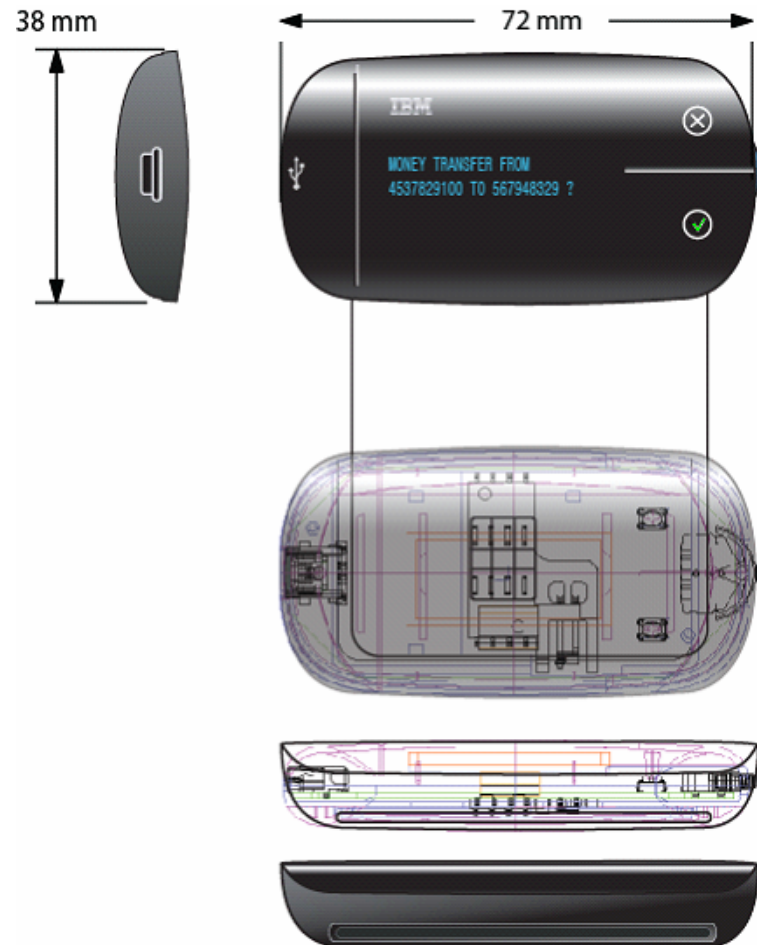
- Due to the immediate TLS link between server and ZTIC
 - (Remote) Administration of ZTIC trivial & without user interaction
 - ZTIC can serve as “remote display” of the server
- Highly configurable system
 - Adaptation to existing solutions possible
 - Proof-of-concept integration of several card-based authentication solutions complete
 - Proxy and on-ZTIC software can be tailored, e.g., to show deployment-specific data
 - EMV CAP + transaction signing has been integrated as proof-of-concept
 - Extension to support/introduce full-blown PKI solution(s)
 - ZTIC operating as a chip card reader, e.g., to digitally sign eMails
 - Adaptation to (perceived) risk setting possible
 - PIN entry on device or on Web page
 - Use of smart card or not
- Existing investments utilizing secure chip cards can be retained
 - Either with ID0 (SIM) or ID1 (credit card) size reader
 - Existing authentication solutions can be augmented to make use of ZTIC display and buttons
 - “Simple” security improvement without overall system changes

IBM Zone Trusted Information Channel (“ZTIC”) Productization

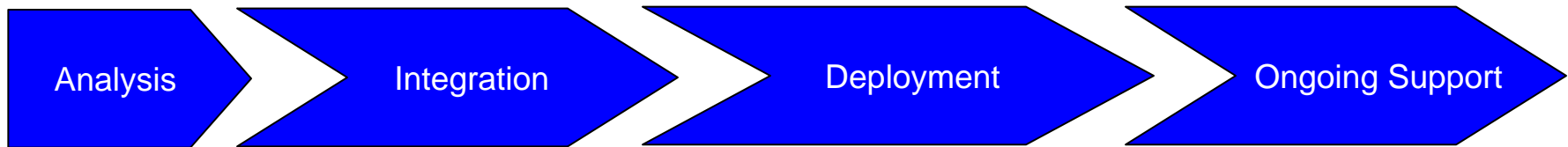


“ZTIC”: Designs

- Primary goals
 - Easy-to-carry (small)
 - Looking respectable on desktop
 - Minimum user interface
 - Allowing for on-device PIN entry
 - Cost-effective manufacturing
- Secondary goals
 - Provide space for (printed) logo
 - Allow for user-provided cabling



“ZTIC”: Phased introduction



- Analysis
 - Test-integration to existing system & initial usability test
- Integration
 - Full integration, possible adaptation of existing system
 - Real-world usability test
- Deployment
 - Design of roll-out device, personalization & deployment methods
 - Delivery of volume orders
- Ongoing support
 - Warranty, 3rd level support and system updates to stay ahead of threats

“ZTIC”: Prices and Timelines

- Price factors
 - Production location
 - Volume
 - Display
 - Warranty & Support conditions
- Current target timeline
 - Q4/08: ZTIC v4 (pilot devices)
 - Q3/09: ZTIC v5 production samples
 - Q4/09: ZTIC v5 volume readiness



Questions?

Michael Baentsch (mib@zurich.ibm.com)
+41 44 724 8620

Zone Trusted Information Channel <http://www.zurich.ibm.com/ztic>
ztic@zurich.ibm.com

