Regulations and Security – An Update

Helmut Bernhard, 13th September 2016
EMEA Senior Solutions Architect

better always on
comforte®

Agenda

- PCI-DSS news
- Regulations and Directives in line with the EU-Digital Single Market strategy
- comForte - Regulations and Security Solutions recap

better always on

comforte®

What is new in PCI-DSS 3.2?

- What is new in PCI DSS 3.2
  - **new sub-requirements for service providers affecting requirements 3, 8 (e.g. multi factor authorisation), 10, 11 and 12.**
  - **Appendix A2 incorporates new migration deadlines for removal of Secure Sockets Layer (SSL) /early Transport Layer Security (TLS) in line with the December 2015 bulletin**
- How long do organisations have to implement PCI DSS 3.2?
  - **PCI DSS 3.1 will retire on 31 October 2016, and after this time all assessments will need to use version 3.2. Between now and 31 October 2016, either PCI DSS 3.1 or 3.2 may be used for PCI DSS assessments. The new requirements introduced in PCI DSS 3.2 are considered best practices until 31 January 2018. Starting 1 February 2018 they are effective as requirements and must be used**
  - **Compensating control for Tokenisation is under stress (not only) due to new EU-regulations**

Digital market initiatives

- EU NIS (Network and Information Security) Directive
  - The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU
- EU GDPR (EU Data Protection Rules Reform)
  - The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business
- eIDAS Regulation (electronic identification and trust services for electronic transactions in the internal market)
  - Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market
- the Revised Directive on Payment Services (PSD2)
  - The PSD II aims at enhancing consumer protection, promoting innovation and improving the security of payment services within the EU

Digital market initiative NIS - Implications

- EU NIS (Network and Information Security) Directive
  - **Status**
    - DRAFT ready May 2016
    - Date of EU vote unknown
    - Date of ratification unknown
- Implications
  - **To early in the review cycle**
  - **complements EU-US Privacy Shield Framework**

Digital market initiative GDPR - Implications

> EU GDPR (EU Data Protection Rules Reform)

  > **Status**

    > Date of EU vote April 2016

    > Date of ratification May 2018

> Implications

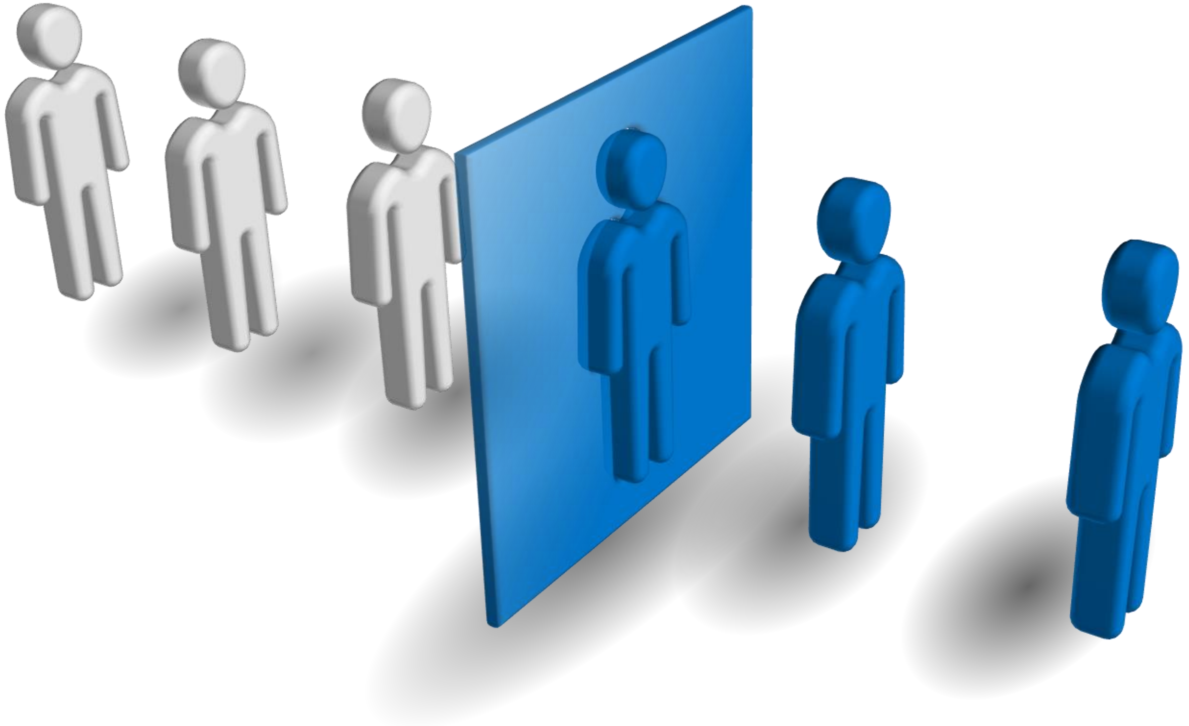
General Data Protection Regulation

The level of risk associated with the GDPR has catapulted data protection into the boardroom

Jane Finlayson-Brown, PARTNER, Allen & Overy, 3/2016

What needs to be done (focus GDPR)

- > Data protection should be included by design within all customer data management implementations (certification needs via EU/national to be selected authorities)
- > Every consumer will have easier access to any data saved about them
- > Every consumer will have the right to know if and when data on or about them has been hacked
- > Every consumer will have the "right to be forgotten," where data can and should be deleted once it is no longer necessary
- > Not meeting these areas can carry a financial penalty of up four per cent of global turnover, which includes all cash revenue that a company generates during a year



cF Focus is → GDPR Security of Processing (Article 30)

- the ***controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk***, including inter alia, as appropriate:
  - **the pseudonymisation and encryption of personal data;**
  - **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;**
  - **the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;**
  - **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.**

DPO Data Processor Officer

Digital market initiatives implications

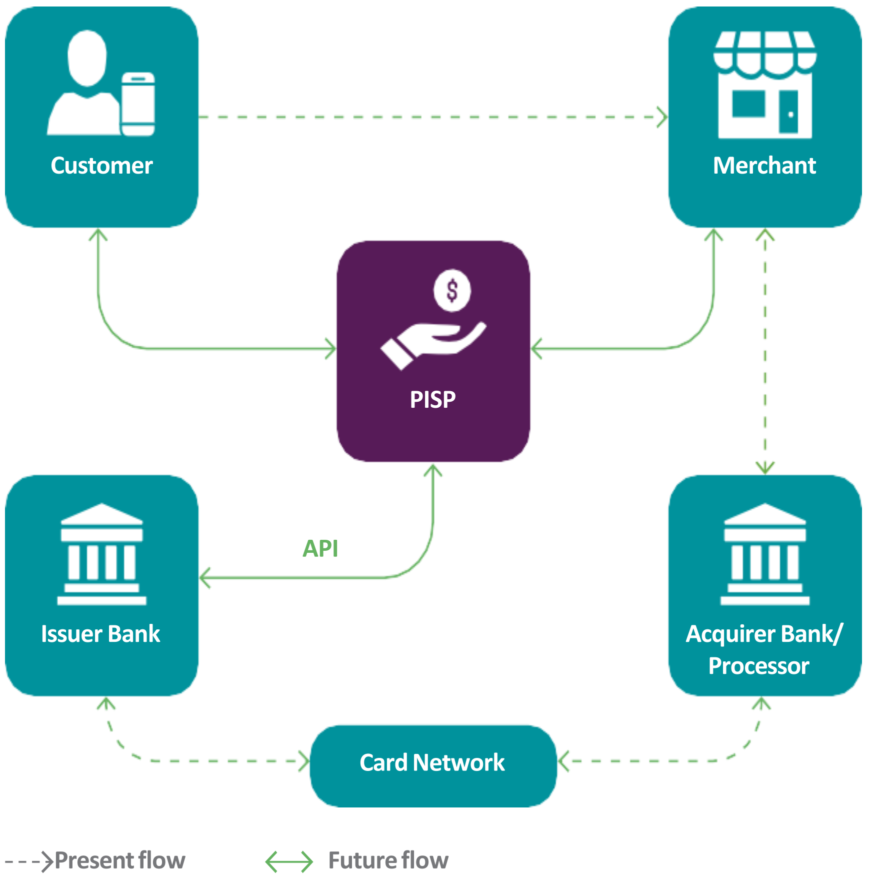
- eIDAS Regulation (electronic identification and trust services for electronic transactions in the internal market)
  - **Status**
    - Date of EU vote July 2014
    - Date of ratification July 2016
- Implications
  - Since July 1, 2016, eIDAS repeals the existing eSignatures Directive, it replaces now any inconsistent national laws in Europe
  - It includes electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication
  - Possible usage for mobile banking 2FA for PSD2 (more to come in 2017)
  - There is no EU-wide certification authority and other trust service provider listed yet from service provider organizations like ETSI

Digital market initiatives

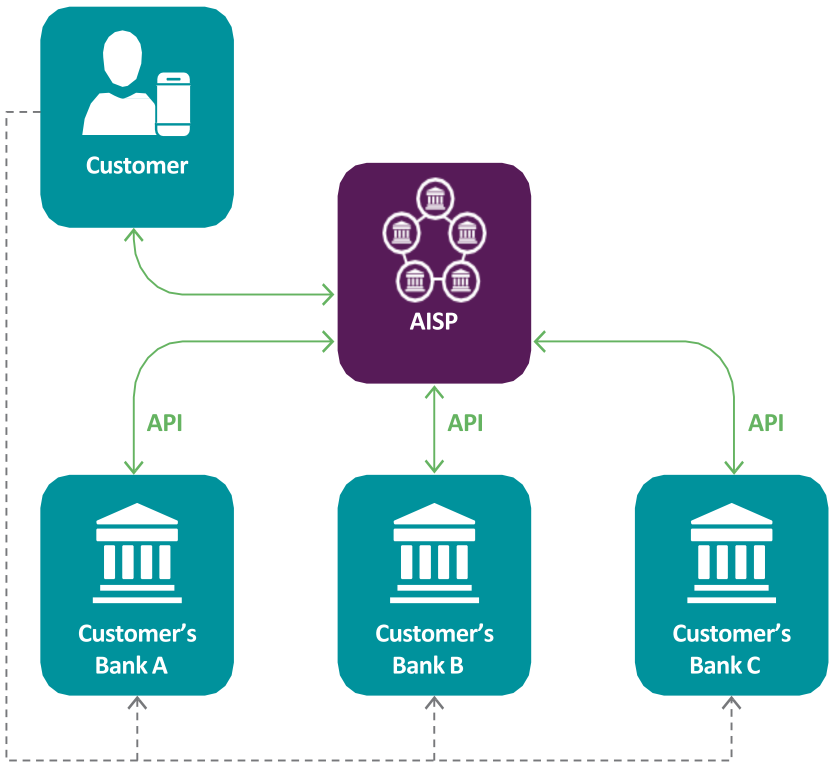
- the Revised Directive on Payment Services (PSD2)
  - **Status**
    - Date of EU vote January 2016
    - Working paper ECB mid of 2017
    - Date of ratification January 2018 (?)
- Complimenting SEPA and PCI-DSS, PSD2 authorizes payment initiators and account information services to officially become payment service providers
- Banks are now called ASPSPs (Account Servicing Payment Service Providers)
- SCA (Secure Customer Authentication) in combination with customer authorisation still unclear, a RTS (Regulatory Technical Standard) expected from the ECB first half of CY2017
- Disruptive “movements” are already here, eg. MC potential purchase of VocaLink, Google bought Apigee (API-ISV)

PSD2 The new disruptive model

AN UPDATED PAYMENT MODEL INCLUDING A PAYMENT INITIATION SERVICE PROVIDER (PISP)

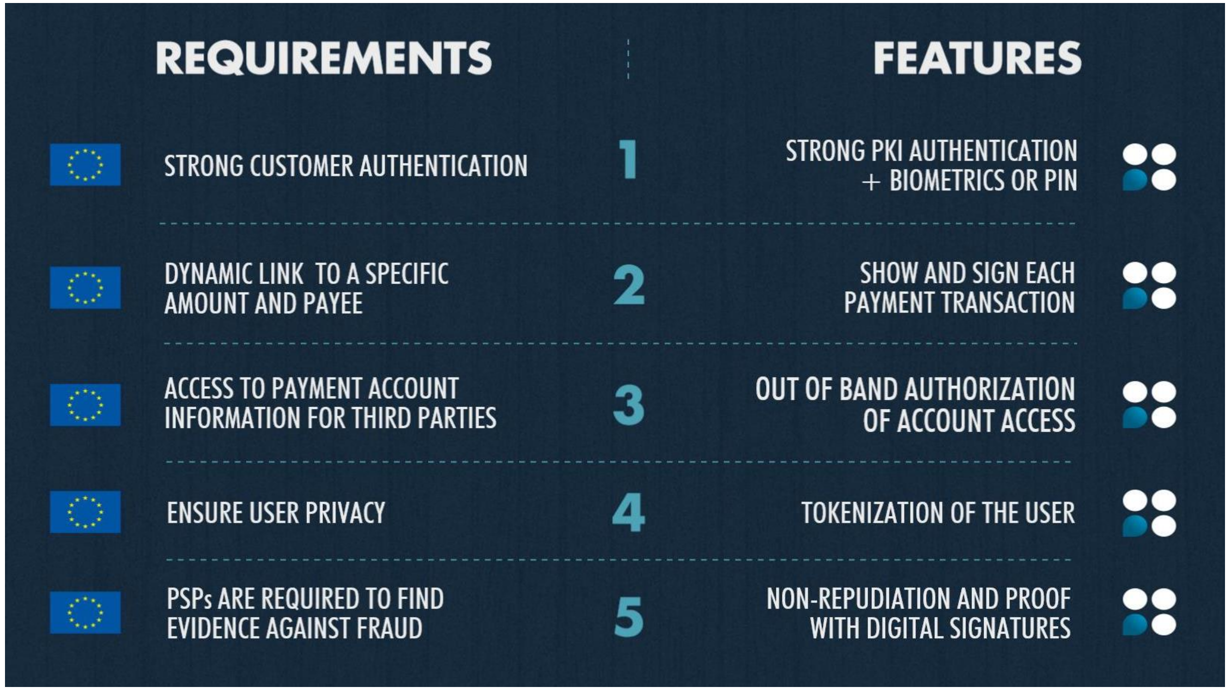


AN UPDATED INTERACTION MODEL INCLUDING AN ACCOUNT INFORMATION SERVICE PROVIDER (AISP)



PSD2 (major changes)

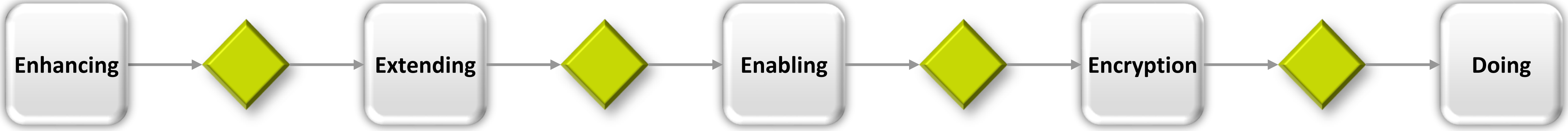
- With PSD2, the Directive will allow retailers to ‘ask’ consumers for permission to use your bank details. Once you give permission, the retailer will receive the payment directly from your bank – no intermediaries
- The direct connection between retailers and banks will be enabled using Application Programming Interface or APIs for short
- The use of API’s is exciting because it enables companies (innovative companies) to connect to financial institutions directly
- With PSD2 they’re introducing Account Information Service Provider or AISP’s, which will allow you to view all of your multi-bank details in 1 portal.
- This is interesting stuff because now it means that current and new providers, not necessarily banks, can consolidate your account information in 1 place and acquire insightful data about you. This offers lucrative cross selling opportunities for these new providers



REQUIREMENTS		FEATURES
STRONG CUSTOMER AUTHENTICATION	1	STRONG PKI AUTHENTICATION + BIOMETRICS OR PIN
DYNAMIC LINK TO A SPECIFIC AMOUNT AND PAYEE	2	SHOW AND SIGN EACH PAYMENT TRANSACTION
ACCESS TO PAYMENT ACCOUNT INFORMATION FOR THIRD PARTIES	3	OUT OF BAND AUTHORIZATION OF ACCOUNT ACCESS
ENSURE USER PRIVACY	4	TOKENIZATION OF THE USER
PSPs ARE REQUIRED TO FIND EVIDENCE AGAINST FRAUD	5	NON-REPUDIATION AND PROOF WITH DIGITAL SIGNATURES

comForte Cybersecurity and Privacy blueprint

> Result oriented Cybersecurity and Privacy innovation process



Enhancing

status quo operation

Without application modifications the different NonStop log files are:

- Collected
- Consolidated
- Condensed
- Merged
- Interpreted

and transferred to a SIEM (e.g. ArcSight)

Extending

the Security architecture

Introduction of:

- KSL (Key stroke logging) for all Nonstop subsystems (e.g. TACL, OSS, Pathway, iTP secure Webserver, etc.)
- Single Sign On connectivity to the rest of customer IT infrastructure

Enabling

a generic Smart Cybersecurity architecture

Transparent end user controlled generic smart interception architecture for:

- $Receive/Pathway
- CGI (also dynamic CGI)
- MBE (Memory based Enscribe)
- Monetisation

Encryption

adaption based on regulations

Encryption and tokenisation is done “under the hood” of the applications.
Usage of:

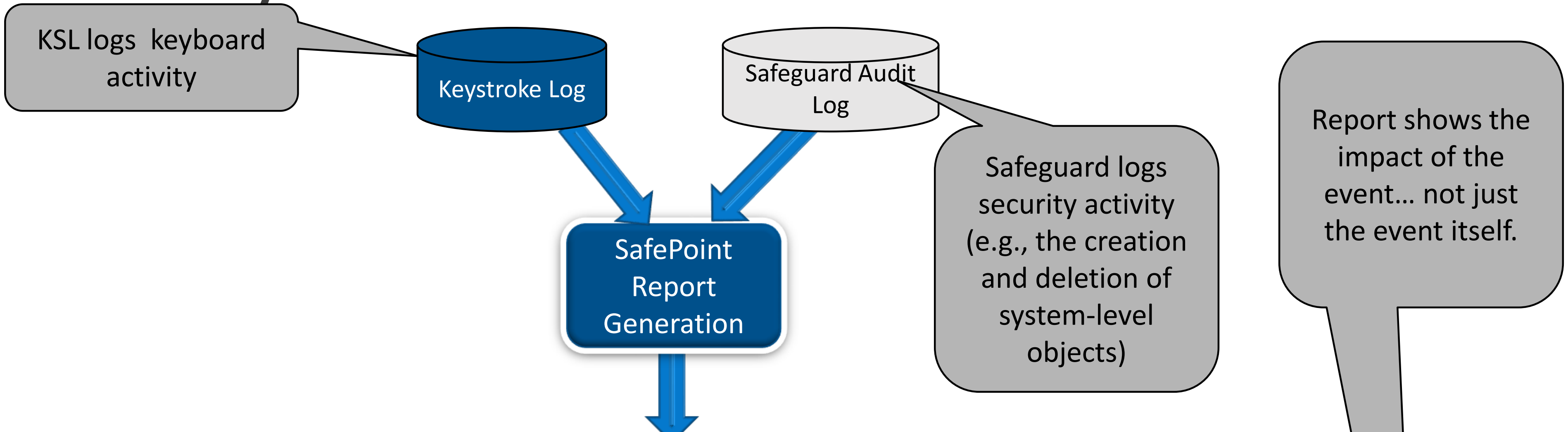
- comForte SSL/TLS products
- Format-preserving field level protection
- Remote files can also be protected
- Multiple format support like PII,PAN,CDR, etc.

Doing

implementation, review and ongoing success control

- Implementation services for the customer
- Launch
- Review
- Performance review
- Ongoing success control

SafePoint/KSL Reports – Merging Keystroke with Safeguard log Report with Keystroke Info



KSL logs keyboard activity

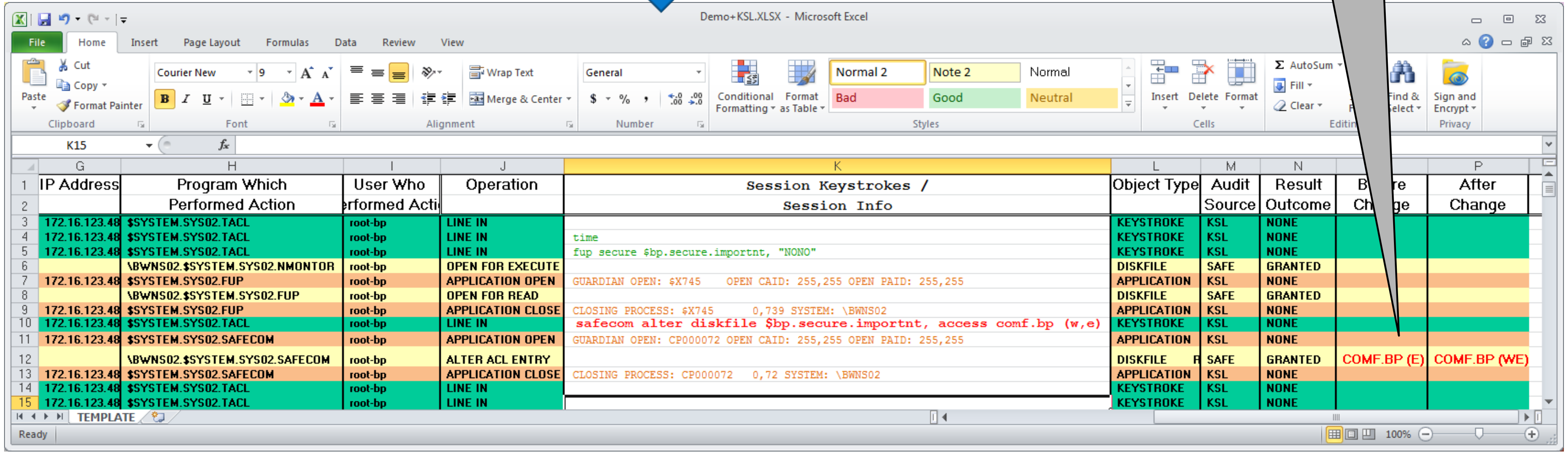
Keystroke Log

Safeguard Audit Log

SafePoint Report Generation

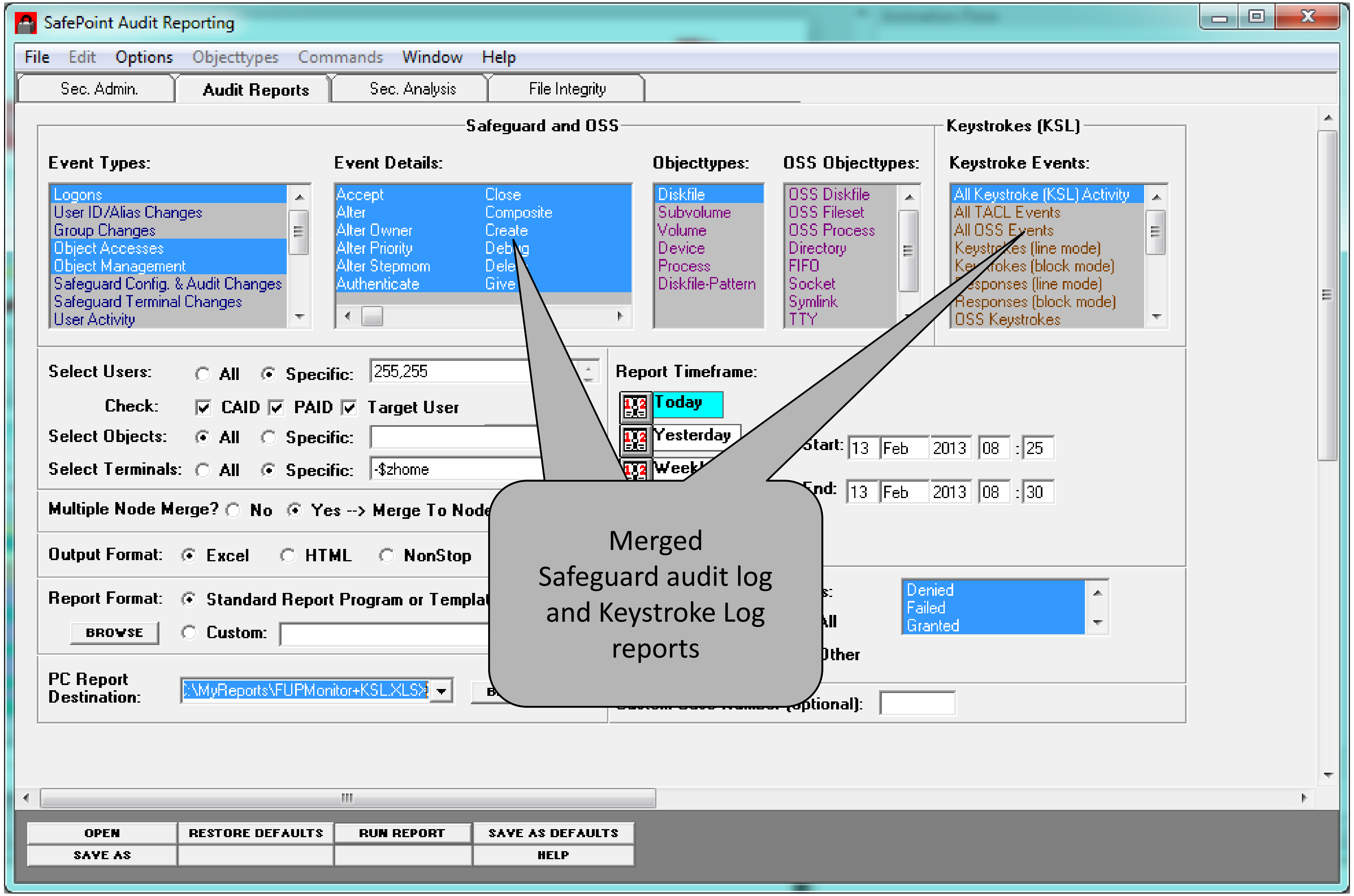
Safeguard logs security activity (e.g., the creation and deletion of system-level objects)

Report shows the impact of the event… not just the event itself.



	G	H	I	J	K	L	M	N		P
1	IP Address	Program Which	User Who	Operation	Session Keystrokes /	Object Type	Audit	Result	B re	After
2		Performed Action	rformed Acti		Session Info		Source	Outcome	Ch ge	Change
3	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN		KEYSTROKE	KSL	NONE		
4	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN	time	KEYSTROKE	KSL	NONE		
5	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN	fup secure $bp.secure.importnt, "NONO"	KEYSTROKE	KSL	NONE		
6		\BWNS02.$SYSTEM.SYS02.NMONTOR	root-bp	OPEN FOR EXECUTE		DISKFILE	SAFE	GRANTED		
7	172.16.123.48	$SYSTEM.SYS02.FUP	root-bp	APPLICATION OPEN	GUARDIAN OPEN: $X745 OPEN CAID: 255,255 OPEN PAID: 255,255	APPLICATION	KSL	NONE		
8		\BWNS02.$SYSTEM.SYS02.FUP	root-bp	OPEN FOR READ		DISKFILE	SAFE	GRANTED		
9	172.16.123.48	$SYSTEM.SYS02.FUP	root-bp	APPLICATION CLOSE	CLOSING PROCESS: $X745 0,739 SYSTEM: \BWNS02	APPLICATION	KSL	NONE		
10	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN	safecom alter diskfile $bp.secure.importnt, access comf.bp (w,e)	KEYSTROKE	KSL	NONE		
11	172.16.123.48	$SYSTEM.SYS02.SAFECOM	root-bp	APPLICATION OPEN	GUARDIAN OPEN: CP000072 OPEN CAID: 255,255 OPEN PAID: 255,255	APPLICATION	KSL	NONE		
12		\BWNS02.$SYSTEM.SYS02.SAFECOM	root-bp	ALTER ACL ENTRY		DISKFILE R	SAFE	GRANTED	COMF.BP (E)	COMF.BP (WE)
13	172.16.123.48	$SYSTEM.SYS02.SAFECOM	root-bp	APPLICATION CLOSE	CLOSING PROCESS: CP000072 0,72 SYSTEM: \BWNS02	APPLICATION	KSL	NONE		
14	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN		KEYSTROKE	KSL	NONE		
15	172.16.123.48	$SYSTEM.SYS02.TACL	root-bp	LINE IN		KEYSTROKE	KSL	NONE		

SafePoint Reports for merged and customized reports



Safeguard and OSS

Event Types:
Logons
User ID/Alias Changes
Group Changes
Object Accesses
Object Management
Safeguard Config. & Audit Changes
Safeguard Terminal Changes
User Activity

Event Details:
Accept, Close
Alter, Composite
Alter Owner, Create
Alter Priority, Debug
Alter Stepmom, Delete
Authenticate, Give

Objecttypes:
Diskfile
Subvolume
Volume
Device
Process
Diskfile-Pattern

OSS Objecttypes:
OSS Diskfile
OSS Fileset
OSS Process
Directory
FIFO
Socket
Symlink
TTY

Keystrokes (KSL)

Keystroke Events:
All Keystroke (KSL) Activity
All TACL Events
All OSS Events
Keystrokes (line mode)
Keystrokes (block mode)
Responses (line mode)
Responses (block mode)
OSS Keystrokes

Select Users: ○ All ● Specific: 255,255

Check: ☑ CAID ☑ PAID ☑ Target User

Select Objects: ● All ○ Specific:

Select Terminals: ○ All ● Specific: -$zhome

Multiple Node Merge? ○ No ● Yes --> Merge To Node

Output Format: ● Excel ○ HTML ○ NonStop

Report Format: ● Standard Report Program or Templat

○ Custom:

PC Report Destination: :\MyReports\FUPMonitor+KSL.XLS

Report Timeframe:
Today
Yesterday
Week

Start: 13 Feb 2013 08 : 25

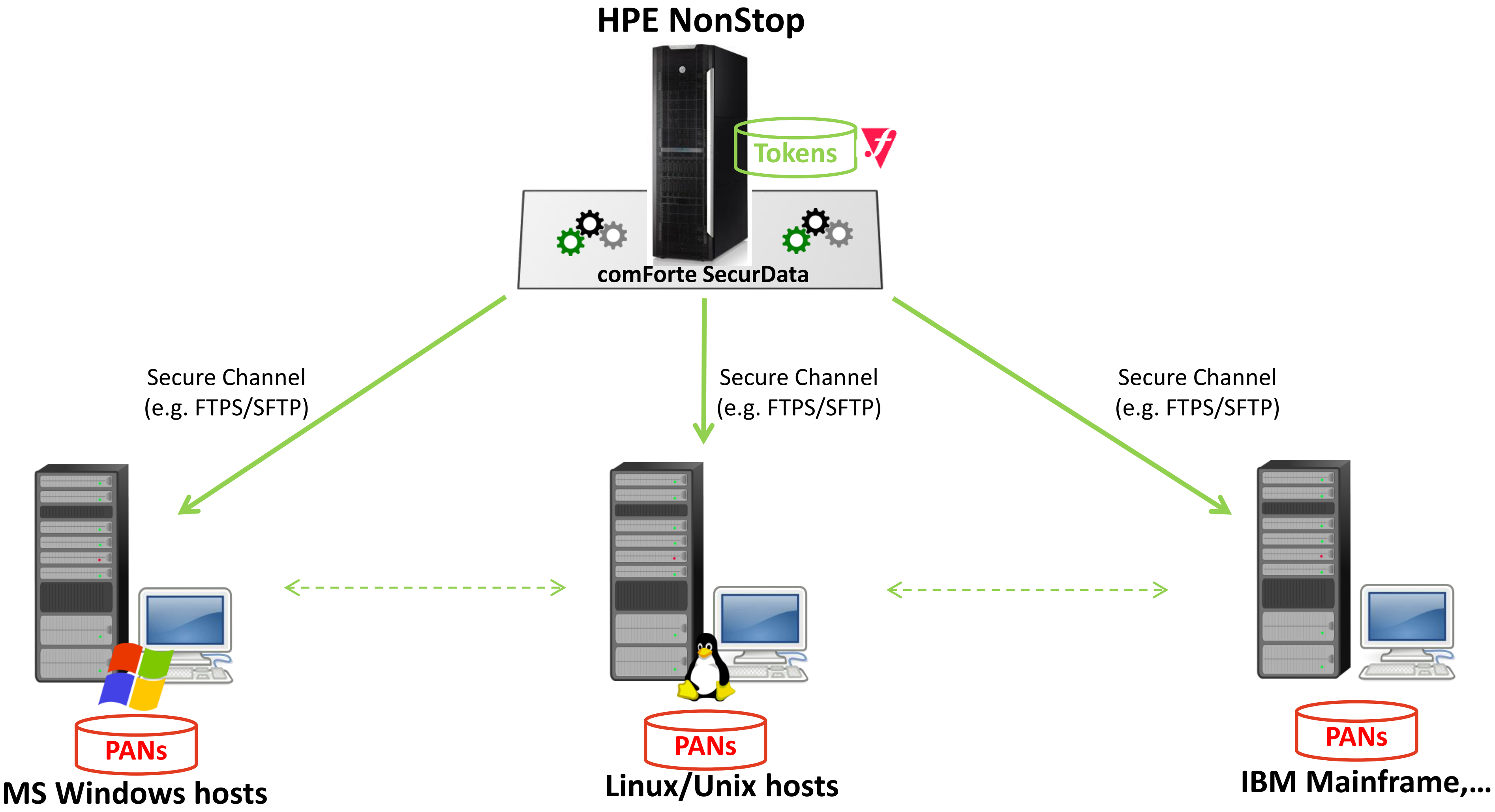
End: 13 Feb 2013 08 : 30

Denied
Failed
Granted

(optional):

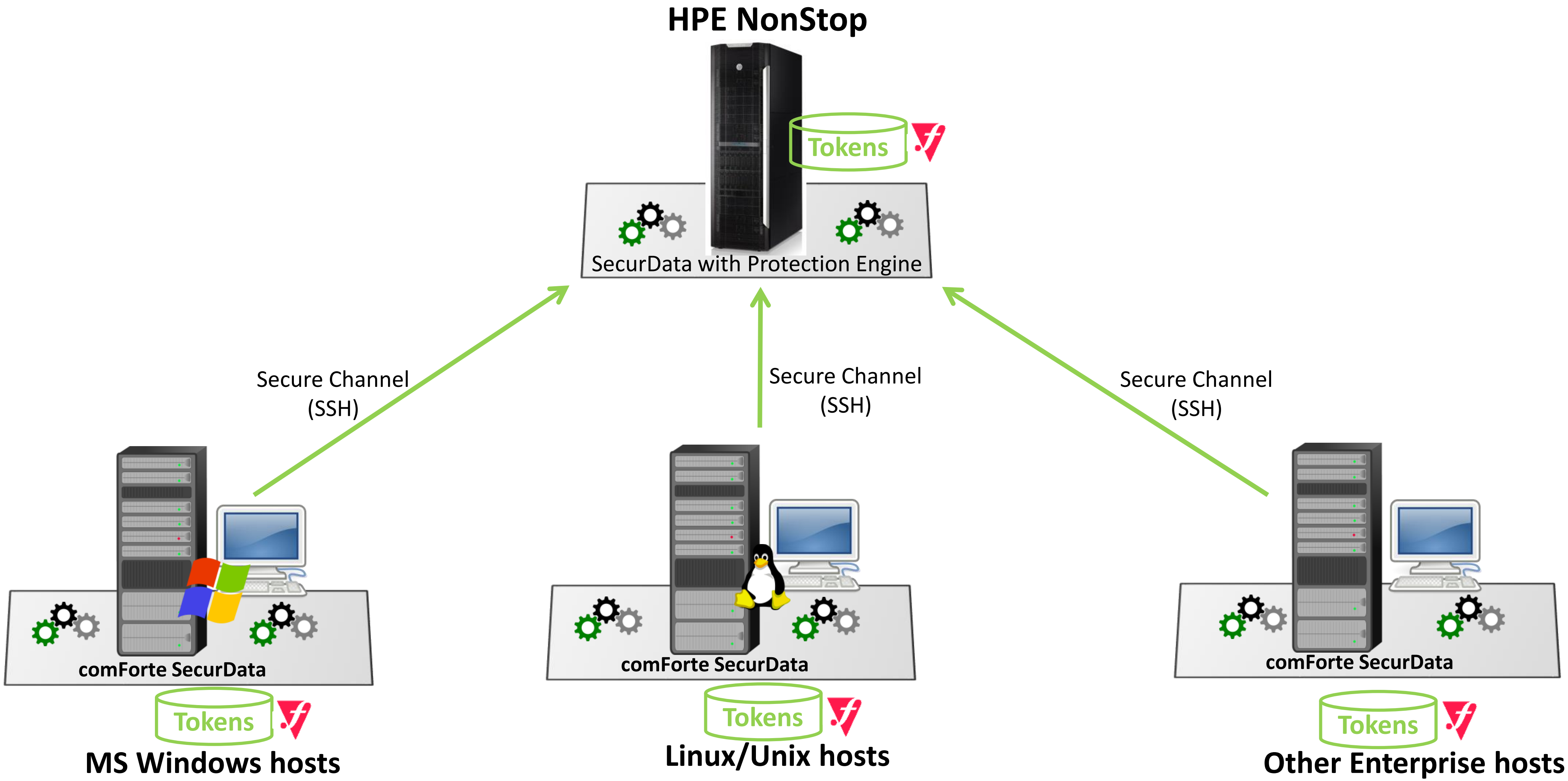
Merged Safeguard audit log and Keystroke Log reports

comForte SecurData On HPE NonStop interoperability



better always on
com.forte®

cF SecurData – NonStop as the tokenization server



better always on

comForte®

Regulations and Security - Recap

- GDPR & PSD2 introduce a lot of data governance obligations
- Use of personal data needs to be scrutinized and justified
- Implementation of appropriate technical and organisational measures, to ensure a level of security appropriate to the risk
- **GDPR is coming, no doubt. May 2018! Start now!**
- Tokenization / Encryption of personal data is key as well as DR
- comForte can help with encryption and tokenization of sensitive/personal data
- Proven solutions / reference customers / lots of experience in the compliance space (e.g. PCI-DSS)

THANK YOU

for your attention!

better always on

com.forte®