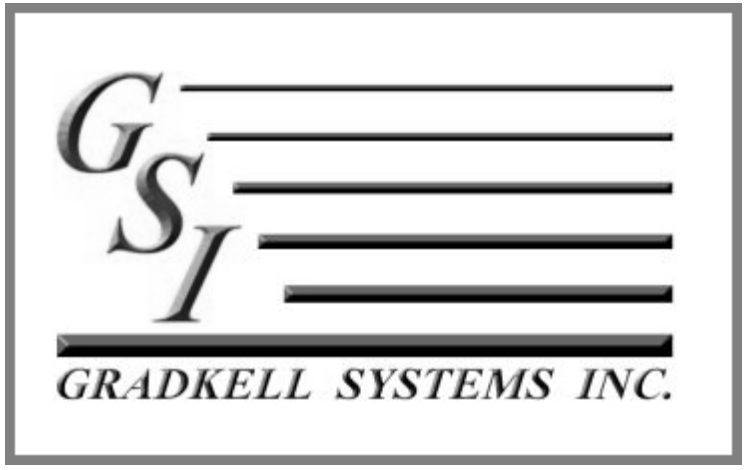
Securing Relational Database Systems with Public Key Digital Signatures

DBsign™ Data Security Suite

by Gradkell Systems, Inc.



Presented to the ***Federal PKI Technical Working Group*** on October 13, 1999

by Mike Prevost of Gradkell Systems

Email: **mprevost@gradkell.com**

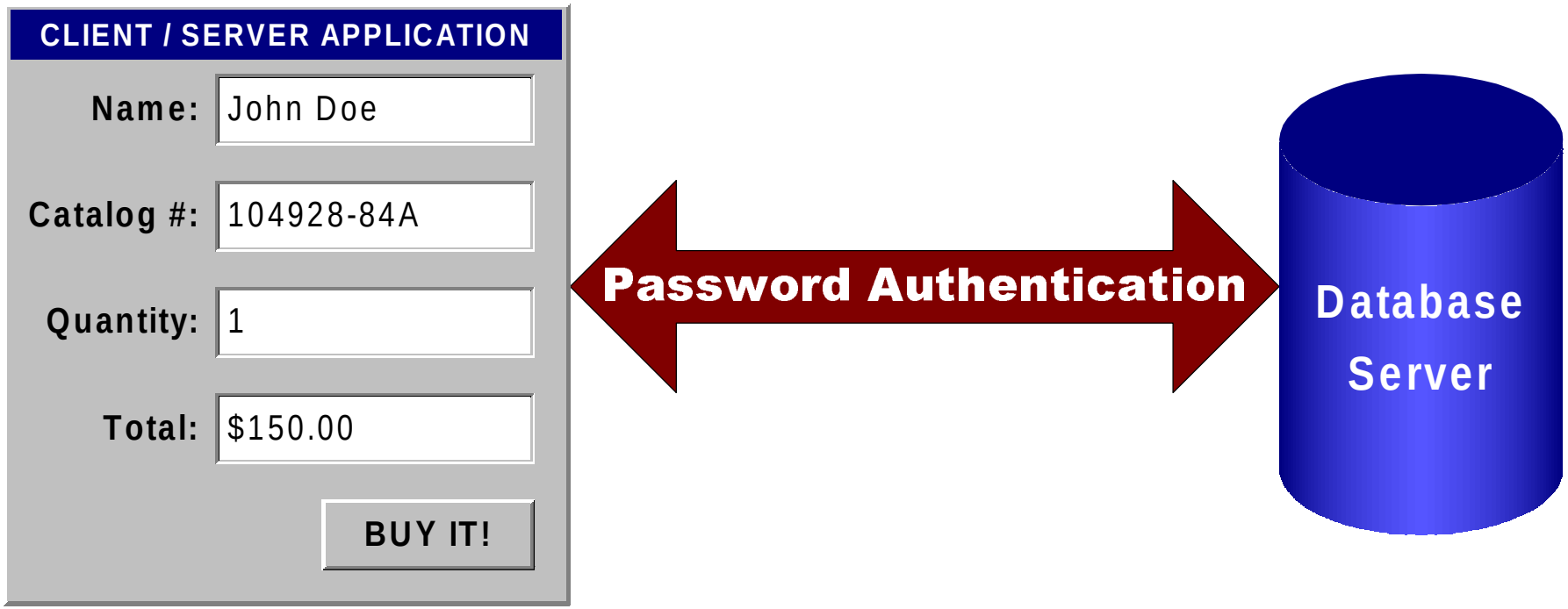
Web Site: **http://www.gradkell.com**

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

About Gradkell Systems, Inc.

- Specialize in paperless database systems
- Largest applications have been paperless financial systems
- Developed first GAO sanctioned paperless disbursing system
- COE has 30,000 smart cards issued world-wide and has disbursed over $27 billion without a paper signature
- Developed the ECS system used by State Dept in all US Embassies to certify, encrypt, and transmit disbursing data between systems (over $5.5 billion disbursed)

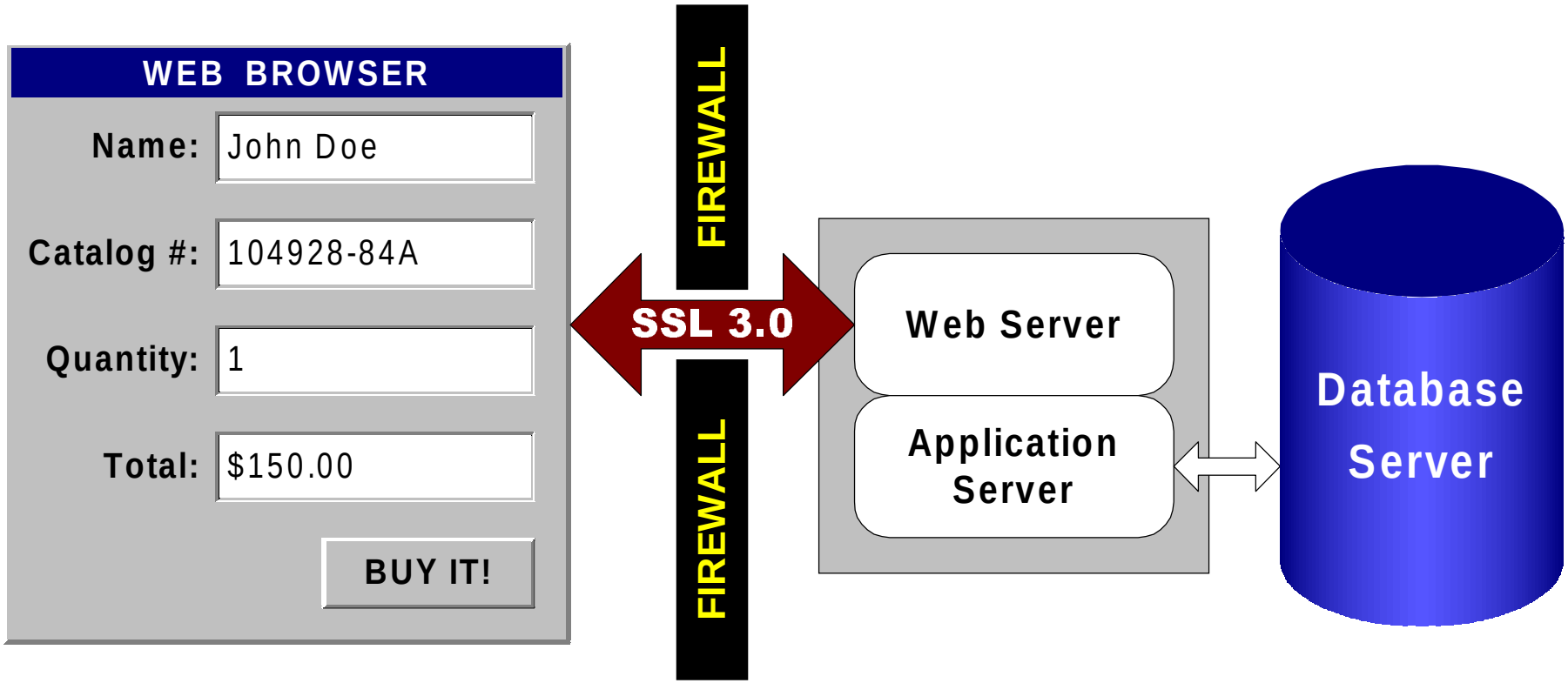
Some Common Architectures



- Typical system before digital signature
- Application code executes on client PC
- Database authenticates user with username/password
- Uses conventional database security mechanisms
- No cryptography

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

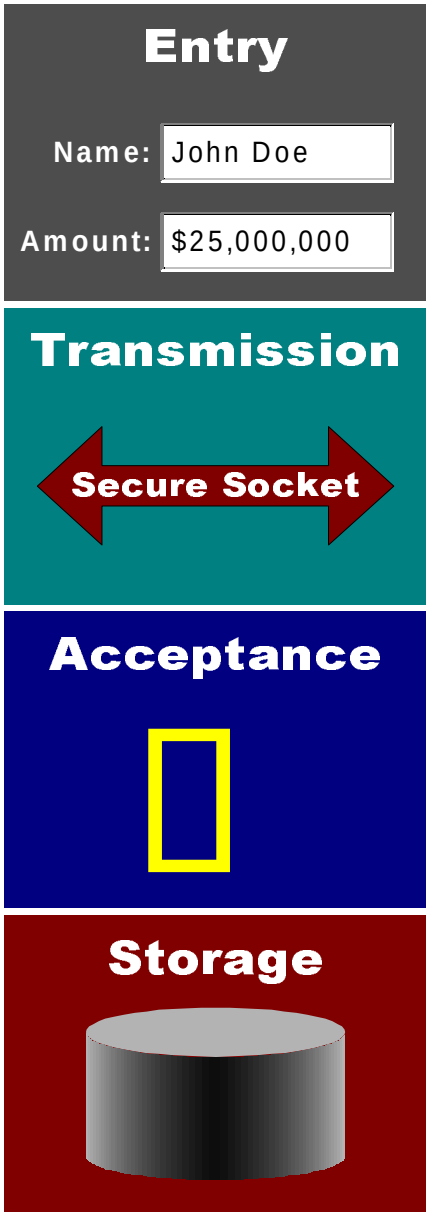
Intranet Web System Using Public Key Technology



- Uses certificate-based authentication via SSL 3.0
- SSL encryption provides privacy during transmission
- Digital signature provides data integrity during transmission
- Transaction protected during transmission only

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

The Four Stages of a Transaction



1. User enters data in application or web browser

2. Transaction data transmitted to database or web server

3. Transaction data accepted by application or application server

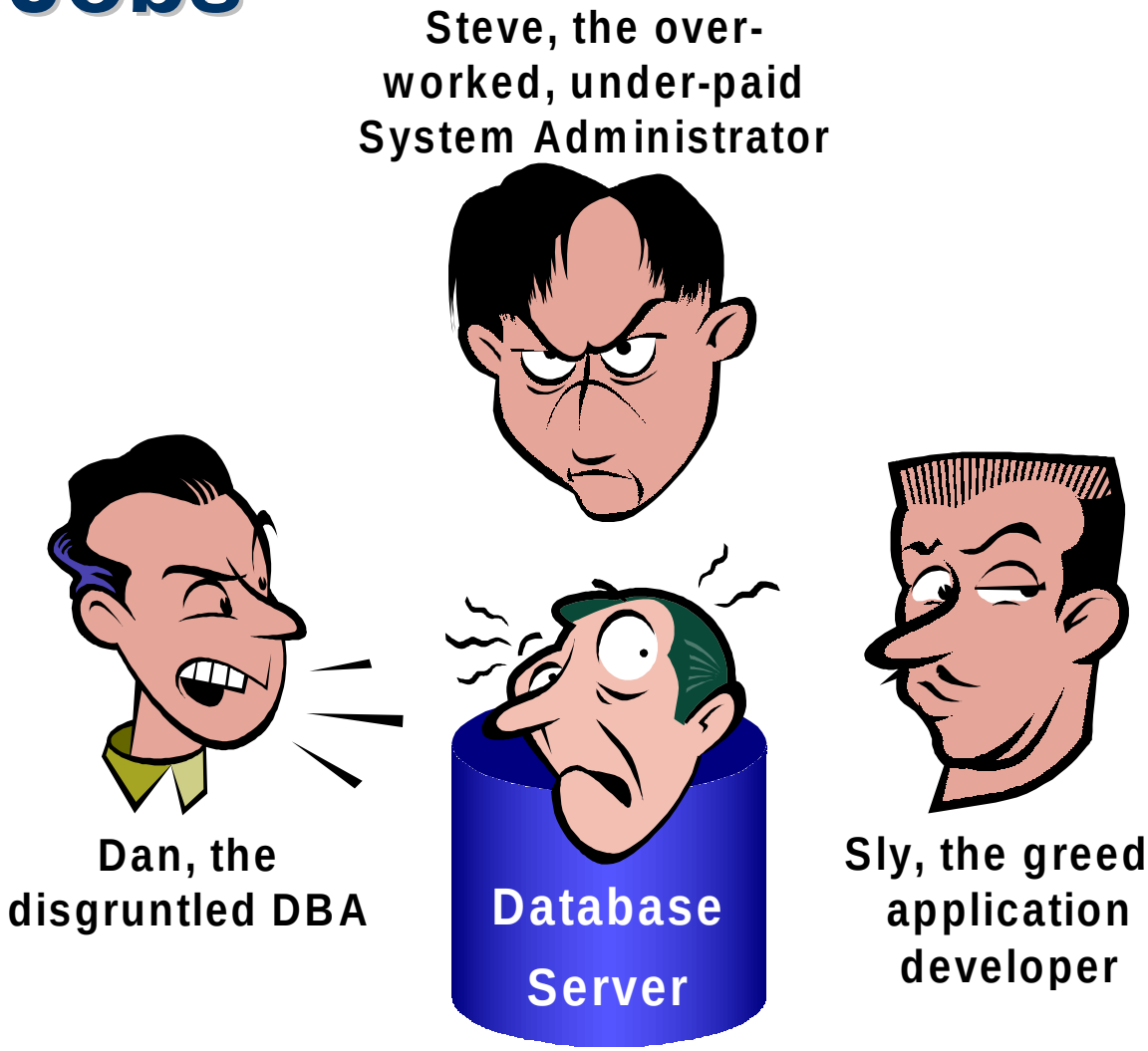
4. Transaction data stored in RDBMS

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

70% to 80% of Computer Crimes are "Inside" Jobs

THE DOMAIN OF EVIL HACKERS

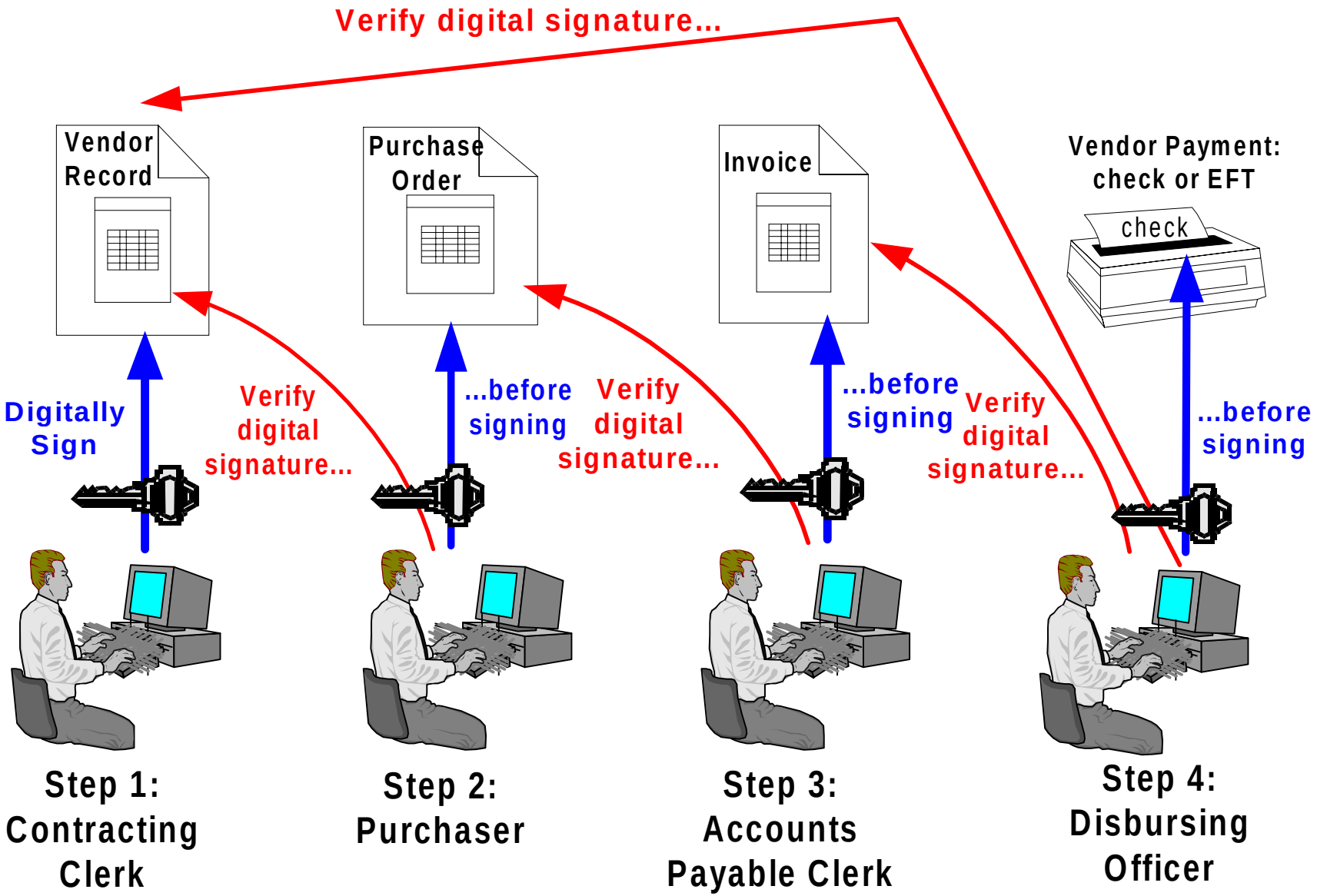
THE MOST SECURE FIREWALL IN THE WORLD



Your data may be more vulnerable than you think!

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

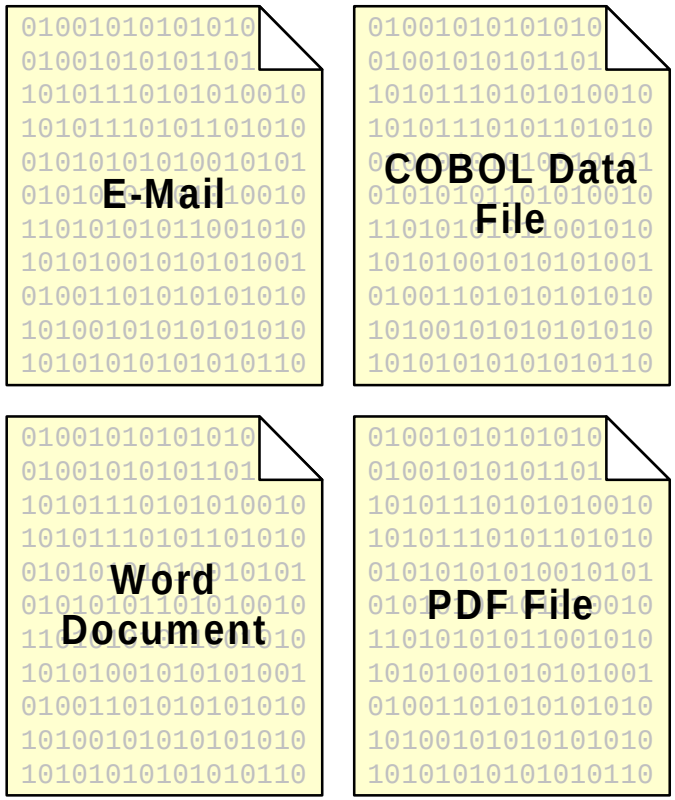
Paperless Business Process



DBSign™ Data Security Suite
by Gradkell Systems, Inc.

Demonstration

What is a Document?



PURCHASE ORDER **#123**

TO: DELL Computer Corporation

FROM: Gradkell Systems, Inc.
4801 University Square, ...

1	4 Processor 600 Mhz Pentium III PowerEdge Server w/ Red Hat Linux	$4,750.00
4	256 MB PC-100 DIMM Memory	$250.00
1	SCSI RAID Controller	$1,750.00
3	24 GB 10,000 RPM SCSI Disk Drive	$1,250.00
1	70 GB DLT Tape Drive	$2,750.00
2	36" High Res Flat Screen Monitor	$6,750.00

Total: $25,764.25

Databases are VERY Different!

Vendor

Vendor Code	Name	Payment Address	...
DM	DELL Computer	1 Dell Way, Round Rock	...
PIZ	Dominos Pizza	Down the Street	...

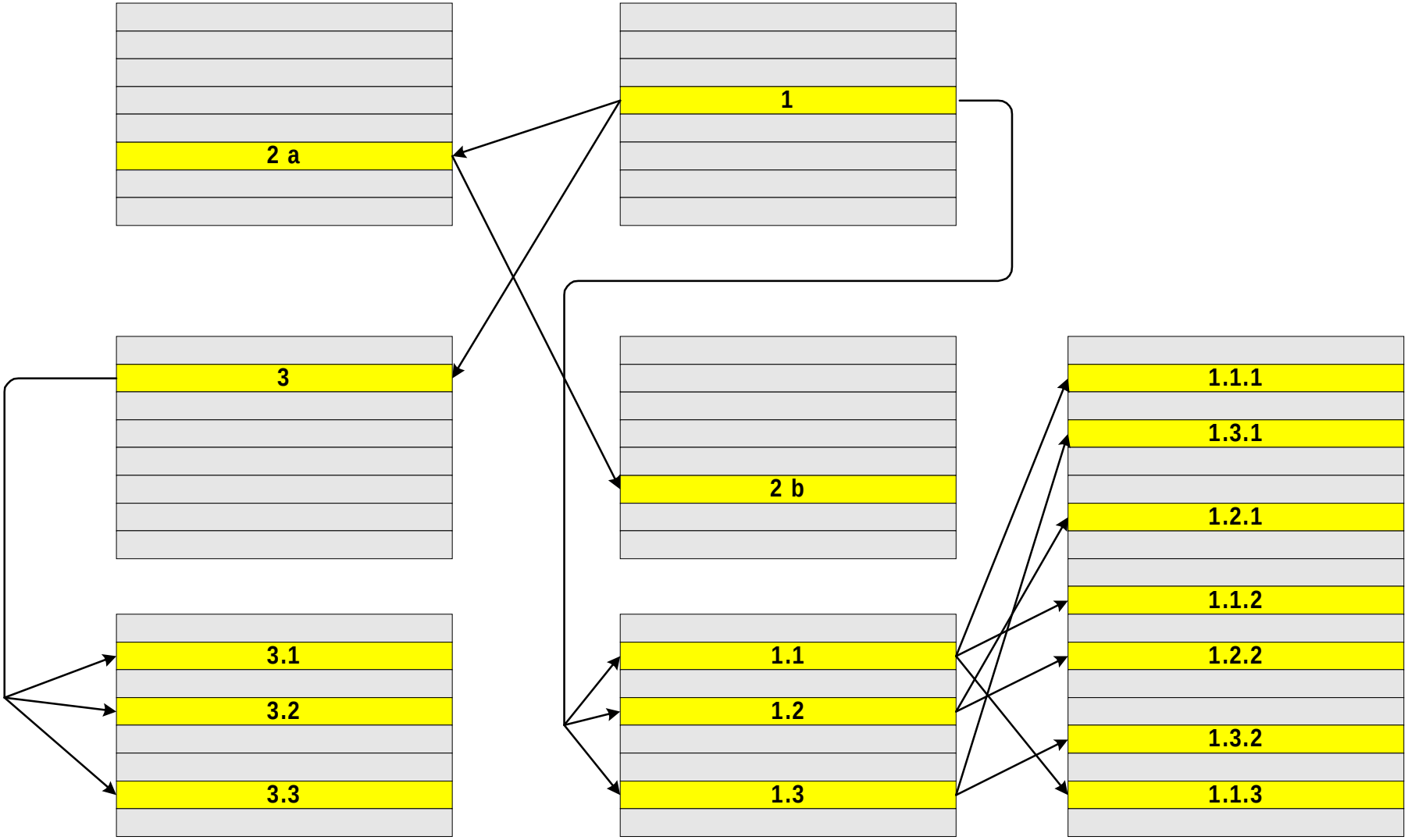
Purchase Orders

P.O. Number	Vendor Code	Approver	Total	...
123	DM	GGASTON	$25,764.25	...
345	PIZ	KGASTON	$27.50	...

P.O. Line Items

P.O. Number	Item #	Qty	Description	Amount	...
123	1	1	4 Processor 600 Mhz ...	$4,750.00	...
123	2	4	256 MB PC-100 DIMM ...	$250.00	...
345	1	2	Large Peperoni +Cheese	$13.75	...

A More Complex Example



The general case can be very complex.

This is not SMIME or SSL Solution

- PKCS #7 based solutions are not optimal in this environment because PKCS #7's are inherently denormalized
  - Storage inefficiencies
    - Duplicate copies of data
    - Duplicate copies of certificates
    - In DoD 10,000 copies of the certificate chain amounts to 249 MB in certificate data alone!
  - Performance risks
  - Security Risks
- Network transmissions are out of scope and can be provided by numerous other products

Digitally signing relational data has unique requirements that are much different from traditional "flat data" solutions.

Current Approaches

Current approaches fall into two categories:

- ***Integration projects using cryptographic toolkits***
  - Require extensive modifications to applications
  - Require a lot of work on the part of applications developers
  - Integration is costly and time consuming
  - Often yields storage, performance, and security problems
  - End result is application specific and difficult to maintain
- ***Development Environments***
  - Examples: “e-Forms” type solutions, HTML form signing, etc.
  - Requires applications be completely redesigned and redeveloped
  - Requires a totally different skill set than traditional development environments
  - Locks you into a specific development environment (and its vendor) for the lifetime of the application

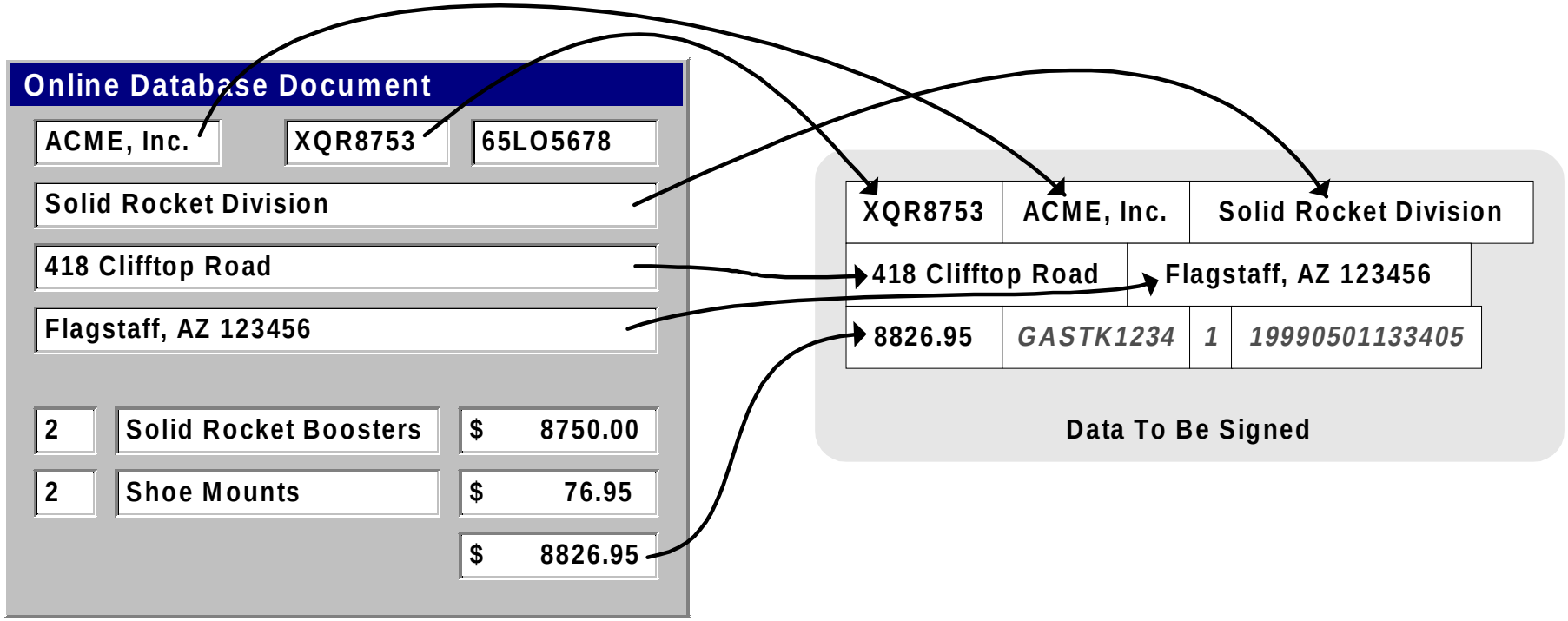
DBSign™ Data Security Suite
by Gradkell Systems, Inc.

DBsign: A Generic, "Data-Centric" Digital Signature Solution

- Solves the general case for signing data in relational databases
- Independent of your database server product and your development environment (not application specific)
- Has zero impact on the structure of your database (only adds tables)
- Very simple to integrate: one line of code per signature operation
- Signature and certificate storage is normalized for efficiency
- Uses digital signature "templates" to allow application designers to specify which data elements are signed.
- Provides audit logging to aid in resolving signature failures

DBSign™ Data Security Suite
by Gradkell Systems, Inc.

Digital Signature Templates



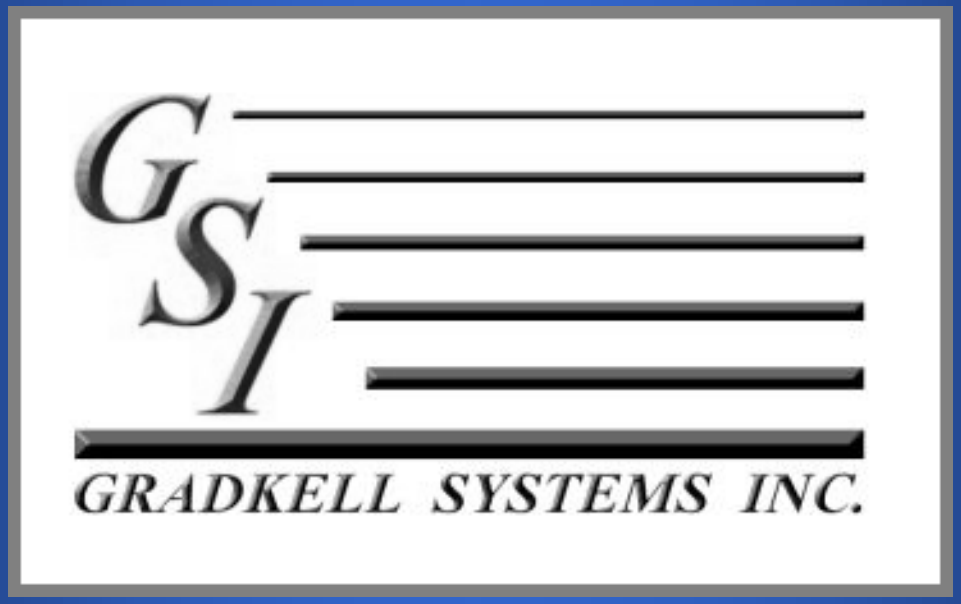
- Specify the database elements that are protected by the digital signature
- Have primary keys and are related to each other in the same way that database tables are related.
- “Versionable” to protect integrity of signatures as data requirements change

Summary

- Databases require a much different solution
- GSI has nearly a decade of experience in this area
- DBsign Data Security Suite
  - is designed from the ground up for relational databases
  - is independent of your development environment
  - is independent of your database product
  - is PKI vendor and PKI token independent
  - provides graphical administration tools
  - provides audit logging features
  - preserves the integrity of your signature throughout the lifetime of your application
  - provides graphical tools to research signature verification failures
  - is very easy to integrate into applications
  - requires little to no training for end users

Questions

(And hopefully answers)


GSI
GRADKELL SYSTEMS INC.