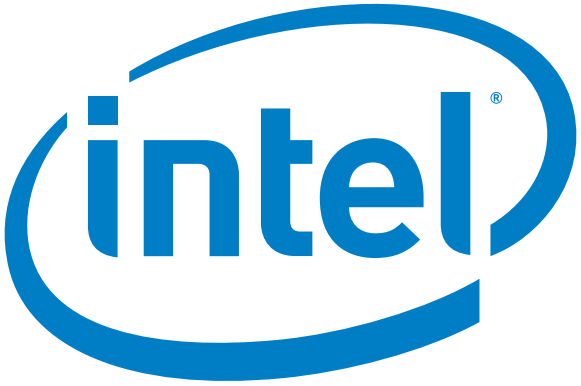


Combating Drug Counterfeiting

Technical and logistical approach

Paul Guermonprez
paul.guermonprez@intel.com

Intel Sofware

August 1, 2007

Goal

- Describe a complete multi-layer solution
- No magical technology or chip to solve the problem
- Show all technical and logistical aspects

Plan

- Main usage models
- Industry, counterfeiter, pharmacist and patient PoV
- Expose sustaining hypothesis
- Describe known risks in detail

Requirements

Needs

Stop a growing public health problem

Counterfeiting is a major health problem, but also a commercial risk for the pharmaceutical industry

Traceability

Traceability may not be a requirement, but is a key ingredient of the solution

Users

Pharmaceutical industry

They produce drugs and packages, firsts steps of logistics

Shipping company

Logistics between industries and pharmacists

Pharmacist

Last step before the patient

Patient

Ideally would like to be involved

Counterfeiters

Equipment

- Factories to produce any kind of package
- Factories to produce RFIDs and barcodes
- Top level IT resources, including security experts

Will

- Capability to punctually steal information from any factory
- Capability to steal information from any shipping company

Scale

Volume of packages

The main metric of the system is the number of packages, let's start with 3.10^9 packages per year per company.

Life of a package

Typically a package information must be available at full speed during the first year, but very long periods are frequent. Consultation of information at reduced speed must be possible for ever.

Basic benchmark

The main criteria for speed in usage models will be the time needed to answer the question "Is this package counterfeit ?".

Evolution

Volume

Volume of packages is expected to grow rapidly. Let's suppose an IT coupled rate of x2 every 18 months.

Information sharing

Several pharmaceutical companies may want to share information about their products, for example after a merging operation. Information systems are independent but must be able to communicate.

Medium

No magical medium

Every medium can be copied, no matter how complicated or proprietary.

Complexity

Small players can't produce complex mediums, counterfeiters can.

Protection comes from accurate information, not the medium.
An open medium will bring more interoperability.

Cryptography

Why ?

Like mediums, every message can be copied.
You can only prevent alteration by signing it.

Who ?

A signature does not worth more than the signer
... and its computer security.

Cryptography will prove a package is authentic, but not unique.
Prevent multiple signers.

Manifest

Informative manifest

We've seen a medium or cryptography alone was not enough, we need to give the package a manifest (description, shipping, unique ID, ...).

Unicity

Copying a signed manifest is easy, but useless if the manifest is so unique you can't sell it many times : The manifest need to contain as much crossable informations as possible.

An unique signed manifest is a first level of verification.

Central traceability

Unique : in theory or in time and space

The central servers will know if the manifest you have is supposed to be at this place and time.

Multiple reads for each package

Inventory in real time of each package at different steps of the supply chain to fill this central repository is now mandatory : high throughput reading technology is needed.

A central traceability is a complementary level of verification. Batch reading problem can be solved by 2D barcodes.

Working together

Several concepts working together :

- A simple medium like 2D barcodes
- A rich manifest, signed by an single authority
- Manifest verified with a central traceability repository

A multi-layer solution,
working for real scale and real complexity problems.

Manifest creation

At the pharmaceutical industry production headquarter :

1. The production planner knows for each of the factories what is the theoretical production planned for the next day.
2. The logistics planner knows where each package is supposed to be shipped.
3. Each package manifest is created : serial number, production, shipping, ...

A manifest is just a simple and unique text, deleting or updating them is not a problem.

Signature creation

At the pharmaceutical industry IT headquarter :

1. The IT secure servers receive the manifests from the planning.
2. They sign the manifests using the unique private key. The information kept in the manifest now can't be changed.
3. Each manifest is entered in the traceability database. But unlike the manifest, the database can be updated.

The private key must remain perfectly protected.
After the signature step, a manifest can't be updated.

Example manifest

Human readable information, standard format :

```
S = FD5S431CD861VG6
N = Plavonsan 75mg
C = 2007-07-09
P = 2009-07-09
DST = EUR/FR/92
```

Example manifest, with signature

Adding an electronic signature, (invisible to humans) :

```
S = FD5S431CD861VG6
N = Plavonsan 75mg
C = 2007-07-09
P = 2009-07-09
DST = EUR/FR/92
-----
owGbwMvMwCTYPN0w8sTRsirGNSlJPLmJeZlpqcUleiUVJW6Td1sEK9gquLn
Gzq7WJgZhrmbcfkBxQJyEssyKxTMTXPTuZyBfCMDA3NdELLkCoBwLaFcl+A
aJC+W5C+pRFXhz0zKwPIaJi9gkwxMxjmacqzNnyslVr7zGpD0YuyxjWatsW
YAqfsD//vFQkw7O0gLXVKu77T3wFAA&=&
=hX74
```

Example manifest, with signature, 2D barcoded

Printing

One label, two parts :

- Human readable : the basic manifest information, in a standard format. Nothing new.
- Encoded in a 2D barcode : the basic manifest information, plus the signature.

With a 2D barcode reader and a small computer :

- Read information at high throughput, verify signature.
- You don't need a computer, a PDA or cellphone is more than enough.

Shipment

Verification

Due to the non alterable nature of the signed manifest, the shipping information on the package can be controlled.

Checkpoints

At the end of the supply chain, a systematic scan of all packages can be done to inventory precisely where each package is, and fill the traceability database.

Barcodes allows large scale batch scanning.
Intermediary inventories are a key aspect of the system.

Delivering

Before delivering : the pharmacist

Just before delivery, the pharmacist can check for the last time the signature is authentic and connect to the pharma industry servers to see if the status of this package is still ok for delivery.

After delivering : the patient

The patient can just do the same at home, with of course less information available, and a manual entry method (or with a cellphone barcode scan).

Barcodes are easy to read, even by patients.

Reconditioning

Simple reconditioning

The barcode of the original package can be easily printed on the smaller container and partial delivery entered in the database.

Complex reconditioning

With a flexible solution, complex scenarios are possible.
Hospitals : Traceability from factory to the patient bed.
Home care : Doctors informed about their patients personal pharmacy.

Barcodes are easy to read and reproduce on demand.
The intelligence is in the network, not the chip.

We suppose

Three hypothesis

1. A perfectly secure server for signatures.
2. Minimum shipping information is known during package creation.
3. Minimum traceability can be done at various steps of the supply chain.

Balance

Note that hypothesis 2 and 3 are balancing : the more you know about shipping at the beginning, the less you need to trace packages, and vice versa.

We do not suppose

- We do not suppose supply chain members and pharmacists are honest. (The system even allows various ways to control their activity . . .)
- Total knowledge of the system definition by counterfeiters is not a risk.
- The open nature of the barcode is not a risk, it is a added value.

The system is able to resist real life conditions.
A little burden for the industry, but a real guarantee.

Initial cost

How much can they spend ?

Research and development done by the counterfeiter to produce the first product. Contrary to other small scale activities, drug counterfeiting industry is able to perform intensive development considering the ROI.

Proprietary or peak technologies are not a long term solution.

Cost of production

Information

Information by itself is not a cost, a complex information won't impact production cost.

Medium

Medium will impact production cost, but it is marginal.
It won't annoy counterfeiters much to produce a 10 cents RFID.

Proprietary or complex mediums won't help.

Conclusions

Keep it simple.

Complex mediums or proprietary formats are not a security, they are just delaying the inevitable a few weeks.

Don't be afraid to open your system, counterfeiters are not afraid of closed systems but users are.

Copy once, ship many

We've seen the authenticity of a package is guaranteed by the network, not only by the signature or the package itself.
Whatever you do, copying a single package and selling it to people not willing to verify anything will always be possible.

Easy and cheap drug counterfeiting, but only works in some areas.
But an informed end user can still verify the product himself.

Copy many, ship many

Unlike multiple copies of a single package, multiple copies of multiples packages are a risk for the system, because they target the official distribution system.
If you can get a copy of the information of all packages in a container you can produce perfect copies and try to sell them on the destination market.

More dangerous, but requires a lot of daily and very specific information to operate : costly.

Shifting interests

In the past counterfeiters had no interest in interacting with the official supply chain or products. Why risk to steal a product if you can produce a fake one for cheap ?
Now the manifests are valuable : you can expect an increased pressure of counterfeiters on the supply chain to steal informations.

You knew counterfeiters in the product age,
prepare yourself to rediscover them in the information age.

Do I need punctual or daily information ?

Punctual

Example : Private part of a signature. Only short term systems rely on this kind of information.

Daily

Example : Signed manifests contents for today's production. Be aware that daily information may be available to counterfeiters.

Limit signatures (ideally one),
daily information will be available,
but make it later than sooner.

Do I need general or specific information ?

General

Example : System or supply chain organization. Like punctual information, keeping general information secret can't be a requirement for a real world system.

Specific

Example : Signed manifest information for packages in my region.

A good system depends upon clarity, not obfuscation.
Leaks of very specific informations are easier to locate and stop.

Logistics

New weak point

We'll see in this document many workarounds, but most of them need an interaction with the logistic chain to get access boxes, not to steal the product itself (useless and heavy) but to copy the information (priceless and light).
The chain will have to support a new pressure and will be the new weak point of the system.

Protect your logistic chain, specially early steps.
If possible, try to separate the product from the packaging.

Bluff

Stay out of the system and bluff

Don't even try to copy a real box, just invent a wrong manifest and false signature.

Easy to do, but very easy to fight

All you need to do is check the signature, not even the central tracking feature.

Generalize a systematic signature checking at multiple steps in the logistic chain.

Large scale, single box multiple copies

Localization of counterfeiting

Copy is easy, but you can't alter the manifest, and the destination is in the manifest.

Easy to do, but easy to fight

Offline signature checking is not enough, you need is use the tracking feature, at least enough to annoy and track resellers. 100% tracking is not possible and not needed.

Offline verification is not enough.
System is useless if you don't use the tracking,
at least part of the time.

Precise copy

Many boxes, copy just a few times

Take frequent samples from the chain and make a small number of copies for each box. You need a frequent access to a lot of boxes (risky), with a preference for unsold boxes.

Localization of counterfeiting

As with large scale copy, the copy is localized.

Protect storage and recycle boxes.
Localize, localize, localize.

Impersonate industry

Not breaking the system

If you have only one signature per pharmaceutical company, you can easily protect it.

. . . just trust in system

But they can easily deploy a parallel system, for example distributing for free a false verification software on internet, or false updates.

Define a single point of rendez vous for information and update before you start deploying.

A single autority is not necessary, the important point is information. Remember the gnupg keys distribution system.

User side

Flooding

Malicious users may flood with innocent requests the servers, causing delayed or no access to other users.

Share access

Users may share their access with counterfeiters.

Attack client computers

Counterfeiters may attack client computer, for example altering the verification software installed, or the verification server connection.

Filter and log accesses to detect unfriendly accesses patterns identify and secure client hardware with VPro technologies

Pharmacist

- The pharmacist will receive with the batch of boxes the information of each box.
- Everything will be loaded in his main software.
- He will receive updates on all boxes in stock in real time.
- He will check a last time when selling the box. It will be the one and only scan of the box (very few manipulations).
- The check will verify the signature and tracking information.
- The tracking information will be updated as “sold“.

Need a computer with barcode and internet access.
Low overhead : only one scan (during the sell), fast (150ms).

Pharmacist - box repackaging

- The pharmacist will receive with the batch of boxes the information of each box, and loaded in the software.
- Repackaging in smaller packages on demand.
- Just printing on a simple sticker with a barcode based on the parent package barcode.
- Update the tracking database with subpackage information.
- Patient at home can access information related to the sub package.

The barcode+tracking system can be adapted to various ways of distribution, including repackaging and hospital pharmacies.

Between industries

- Each industry has its own sensitive tracking information in house.
- Each industry has its own private signature.
- Sharing of simple and atomic information is easy.
- The data format and standard is easy to implement for all.
- The way to access atomic information is highly scalable.

Total autonomy, not expensive, simple, scalable.

New industry joining the system

- Need a trusted signature from other pharmaceutical companies.
- Just reuse the existing deployment infrastructure.
- The data format and standard is easy to implement for all.

Expandable system, fits to a changing world.

Patient - Trusted environment

- The pharmacist is checking the package in front of you.
- The pharmacist software keeps track of patient : you receive automatically alerts on your phone and email.
- You receive the package and bring it home.
- You enter manually the package serial number in a private web interface : you receive automatically alerts.
- You have a simple and private way to keep track of your medicines, should you want to share this information with your doctor.

Building trust between you and your pharmacist, the industry.
You are not only a consumer,
you are informed and part of the solution.

Patient - Untrusted environment

- You get a box on a market in a remote area from non medical personnel.
- You use your cellphone camera to read the barcode and check the signature. A simple software is checking it.
- If the signature is OK, you then verify than dates and destination fit your time and location.
- If yes, your cellphone is sending the serial number to a central service by SMS for verification.
- You receive by SMS a few seconds later the answer : yes this box is unique as far as we know and is not reported as already sold or as a counterfeited product.
- The tracking information is updated as sold.

Flexible system, even works in untrusted environments with a simple camera cellphone.

Emergency worker

- You receive random batches of medicine from all over the world without additional tracking information.
- You scan the packages, check the signatures (you don't filter the destinations because of the varied origins).
- You have a small listing of all serial numbers for interesting references and for each of them a simple status : yes/no. A 160grams typical mp3 player can store 150 billions of these records.
  You check the serials against this database.
- Each week an update stored on a flash drive is received with the weekly arrival of supplies from the capital where they have intermittent access to internet to download updates to the listing.

No more than a week far from the updated information.
Totally offline usage model, works for large quantities.

Needs

Scope

Medical information is extremely sensitive and should be handled by authorized personnel and information systems. Such systems, under the laws of the country and the will of the patient could share information. To do so they need common data formats. These formats collect only minimal information, they do not replace the complete electronic medical records.

Data formats

- Drug Packaging Information
- Patient Information (not an electronic medical record)
- Personal Pharmacy (not your current medications)

Drug Packaging Information

- Pharmaceutical Industry Name, 2 alpha characters ASCII
- Unique number (for the Pharmaceutical Industry), unsigned 64bits integer
- Brand name, ASCII
- Active substance, ASCII
- Pharmaceutical form, ASCII
- Production date, iso format
- Expiry date, iso format
- Geographical destination, with 2-3 ASCII caracters tokens from large to small scale, separated by hyphens
- GnuPG Signature of all informations signed by the Pharmaceutical Industry private key, not mandatory

Drug Packaging Information - Example

- Pharmaceutical Industry Name : “SA” for “Satis Anovis”
- Unique number : “2136545645 6”
- Brand Name : “Dolipronax”
- Active substance : “paracetamol”
- Pharmaceutical form : “capsula”
- Production date : “2007-12-24”
- Expiry date : “2009-12-24”
- Geographical Destination : “EU-FR-PAR-HL” for Hopital Lambda in Paris, France, Europe. Could have be “EU-FR-PAR” or “”EU-FR“”

Drug Packaging Information - XML Schema

```
<?xml version=‘‘1.0’’ encoding=‘‘UTF-8’’?>
<xsd:schema xmlns:xsd=‘‘http://www.w3.org/2001/XMLSchema’’
        targetNamespace=‘‘http://www.intel.com/schema/MedicineXMLSchema’’
        elementFormDefault=‘‘qualified’’>

    <xsd:element name=‘‘drugpackaging’’>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name=‘‘industry’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘serial’’ type=‘‘xsd:double’’/>
                <xsd:element name=‘‘brand’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘substance’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘form’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘production’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘expiry’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘destination’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘signature’’ type=‘‘xsd:string’’/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
</xsd:schema>
```

Drug Packaging Information - XML Data Example

```
<?xml version=‘‘1.0’’?>
<drugpackaging language=‘‘en’’>
        xmlns=’http://www.intel.com/schema/DrugPackagingXMLSchema’
        xmlns:xsi=’http://www.w3.org/2001/XMLSchema-instance’
        xsi:schemaLocation=’http://www.intel.com/schema/MedicineXMLSchema drugp

        <industry>SA</industry>
        <serial>21365456456</serial>
        <brand>Dolipronax</brand>
        <substance>paracetamol</substance>
        <form>capsula</form>
        <production>2007-12-24</production>
        <expiry>2009-12-24</expiry>
        <destination>EU-FR-PAR-HL</destination>
        <signature>owGbwMvMwCTYPNOw8sTRsirGNSlJPLmJeZlpqcUleiUVJW6Td1sEK9gquLmY

</drugpackaging>
```

Patient Information

- First Name, UTF-8
- Last Name, UTF-8
- Sexe (M/F)
- Date of birth, ISO
- Date of death, ISO
- Height (float, kilograms)
- Weight (float, meters)
- Blood type
- Allergies
- Notes

Patient Information - Example

- First Name : Paul Franois
- Last Name : Guermonprez
- Sex : M
- Date of birth : 1977-07-12
- Date of death : null
- Height : 184
- Weight : 84
- Blood type : null
- Allergies : null
- Notes : null

Patient Information - XML Schema

```
<?xml version=‘‘1.0’’ encoding=‘‘UTF-8’’?>
<xsd:schema xmlns:xsd=‘‘http://www.w3.org/2001/XMLSchema’’
        targetNamespace=‘‘http://www.intel.com/schema/MedicineXMLSchema’’
        elementFormDefault=‘‘qualified’’>

    <xsd:element name=‘‘patientinformation’’>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name=‘‘first’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘last’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘sex’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘birth’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘death’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘height’’ type=‘‘xsd:float’’/>
                <xsd:element name=‘‘weight’’ type=‘‘xsd:float’’/>
                <xsd:element name=‘‘blood’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘allergies’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘notes’’ type=‘‘xsd:string’’/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
</xsd:schema>
```

Patient Information - XML Data Example

```
<?xml version=‘‘1.0’’?>
<patientinformation language=‘‘fr’’>
        xmlns=’http://www.intel.com/schema/PatientInformationXMLSchema’
        xmlns:xsi=’http://www.w3.org/2001/XMLSchema-instance’
        xsi:schemaLocation=’http://www.intel.com/schema/MedicineXMLSchema patie

        <first>paul franois</first>
        <last>guermonprez</last>
        <sex>M</sex>
        <birth>1977.07-12</birth>
        <death></death>
        <height>184</height>
        <weight>84</weight>
        <blood></blood>
        <allergies></allergies>
        <notes></notes>

</patientinformation>
```

Personal Pharmacy

- Package Information : Pharmaceutical Industry Name, 2 alpha characters ASCII
- Package Information : Unique Number, unsigned 64bits integer
- Package Information : Expiry Date, iso format
- In date, iso format
- Out date, iso format
- Content Remaining, percentage 0-100, unsigned integer

Personal Pharmacy - Example

- A box of Dolipranox “SA 21365456456”
- expiring 2009-12-24 (date is a cross check)
- bought 2007-10-01
- with 3/8 pills remaining (37%)

Personal Pharmacy - XML Schema

```
<?xml version=‘‘1.0’’ encoding=‘‘UTF-8’’?>
<xsd:schema xmlns:xsd=‘‘http://www.w3.org/2001/XMLSchema’’
        targetNamespace=‘‘http://www.intel.com/schema/MedicineXMLSchema’’
        elementFormDefault=‘‘qualified’’>

    <xsd:element name=‘‘personalpharmacy’’>
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element name=‘‘industry’’ type=‘‘xsd:string’’/>
                <xsd:element name=‘‘serial’’ type=‘‘xsd:double’’/>
                <xsd:element name=‘‘expiry’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘in’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘out’’ type=‘‘xsd:date’’/>
                <xsd:element name=‘‘remaining’’ type=‘‘xsd:int’’/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
</xsd:schema>
```

Personal Pharmacy - XML Data Example

```
<?xml version=‘‘1.0’’?>
<personalpharmacy language=‘‘fr’’>
        xmlns=’http://www.intel.com/schema/PersonalPharmacyXMLSchema’
        xmlns:xsi=’http://www.w3.org/2001/XMLSchema-instance’
        xsi:schemaLocation=’http://www.intel.com/schema/MedicineXMLSchema perso

        <industry>SA</industry>
        <serial>21365456456</serial>
        <expiry>2009-12-24</expiry>
        <in>2007-10-01</in>
        <out></out>
        <remaining>37</remaining>

</personalpharmacy>
```

Legal

Copyright

GNU Free Documentation License

Other Copyrights

Contact

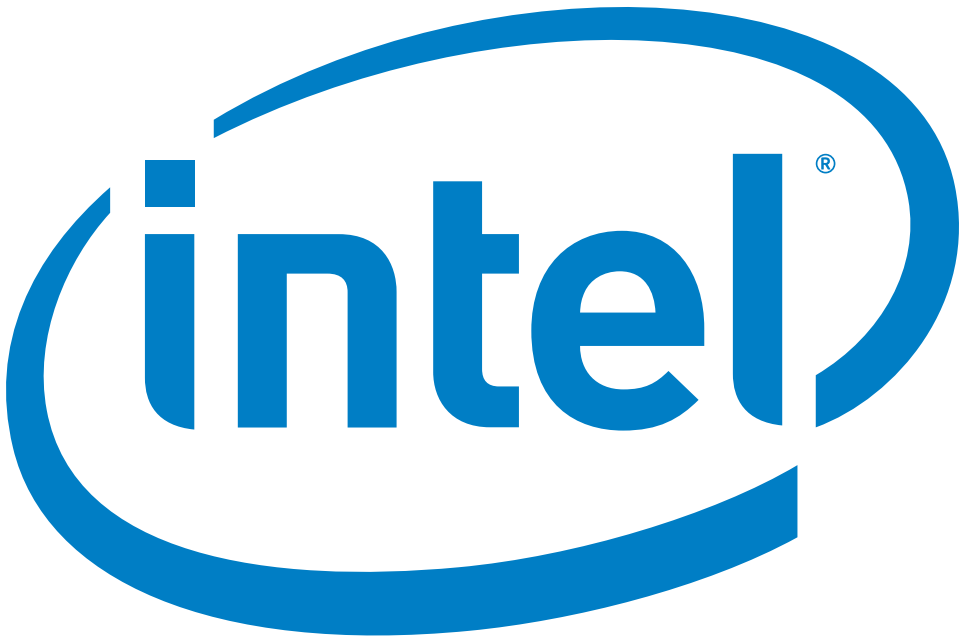
Contact

Paul Guermonprez - Intel
2 rue de Paris, 92196 Meudon, France
paul.guermonprez@intel.com

Versions

Versions

- 2007-08-01 : Initial version.


intel


intel