Discover innovative IT Security Solutions with excellent ROI for your company
XRayWatch
DeviceWatch
Unlimited Device Management
DEvCon
CDWatch
CD & DVD
Cost-efficient
Controlled
Secure
Protect
Confidentiality
PDWatch
itWatch
...and you see EVERYTHING
Discover innovative IT security Solutions with excellent ROI for your company

# SECURE DEVICE MANAGEMENT CREATES COST REDUCTION FOR THE BAVARIAN POLICE

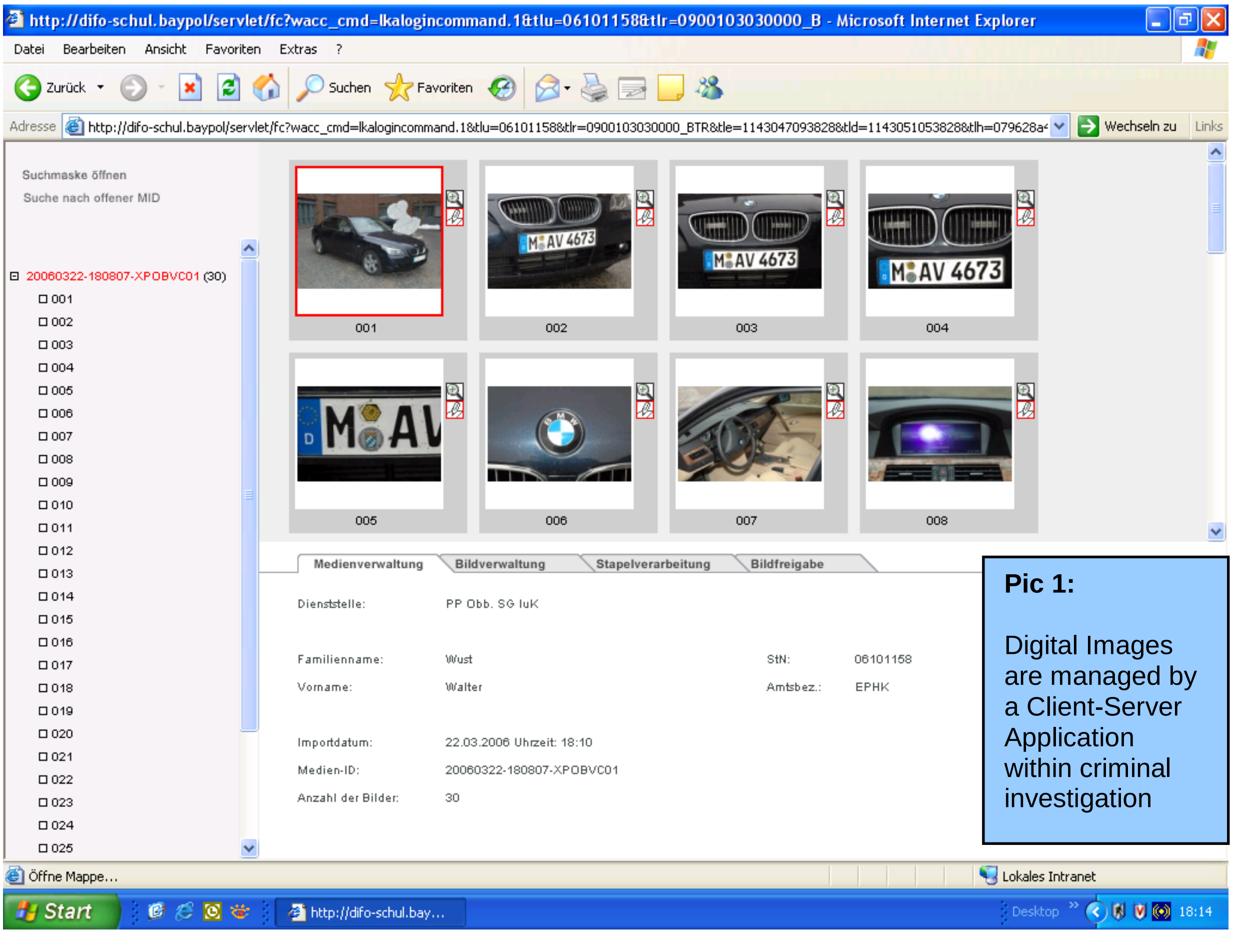
## A PROJECT REPORT

**The project “Digital Photography” of the Bavarian Police shows the cost savings potential of new technologies, e.g. digital cameras. The expensive methods of traditional photography at the site of crimes with analog cameras and following negative and picture development are a thing of the past, at least in Bavaria. The cost advantage does not only apply to the production of the pictures but also has a positive effect on the whole life cycle and the defined processes. The quick – if necessary – federal availability of digital photographs is, especially in the year of the soccer world cup, a further main advantage compared to former methods. This approach puts Bavaria in a leading position where it defines standards that will not only serve many authorities and businesses. For this reason, the key factors of the “Digital Photography” project will be worked out here in detail and the key function that the product DeviceWatch takes on in this context will be closely described.**

**The project “Digital Photography”** – in the following called DiPho – is closely linked to the area-wide availability of the operating system Microsoft Windows XP. Under Windows XP peripheral devices – in the following referred to as simply “devices” – may be simply utilized with the “Plug and Play Technology”. Here, the interfaces of USB, FireWire, PCMCIA, Bluetooth and others may be used in order to connect the devices to the PC workstation. The utilization obviously brings certain risks with it which have been previously described in detail in [Sch04] and [Sch05].

Actually, the Bavarian Police utilize approximately 20,000 PCs. All computers have been equipped with the latest operating system Windows XP in 2005 within a few months. Soon after the introduction, the project requirements included the ability integrate digital cameras. It turned out to be a key factor that is oftentimes forgotten by other authorities during the roll-out plans. This early communication between the basis project “Operating System” and the user project “DiPho” was critical for the efficient implementation in all projects.

**From the IT platform perspective** – i.e. the operating system and system related components – the most secure operation is characterized by the turn-off of all interfaces with “board tools”. “Board tools” are here Group Policy objects (abbreviated as GPOs), the BIOS and local set-ups (e.g. the right to certain registry keys via access control lists.) With the introduction of the project “DiPho” the Bavarian Police actually have the need to open the platform’s interfaces – naturally only for the pre-defined utilization. A first method of resolution was to agree upon a strictly defined procurement process for hardware with central validation and approval including peripheral devices.  Soon, market analysts saw that the speed in which the market for peripheral devices was changing, within the centrally managed approval process could not be implemented as necessary. Due to the fact that cost pressure and improved flexibility were the main reasons for the realization of the project “DiPho” it would have been counterproductive to exclude realistic cost saving potentials from the beginning. The cost of comparable digital cameras underlies a constant downtrend. Therefore, models with technical improvements or new functions are often launched under a new name which avoids time intensive central validation



Adresse: http://difo-schul.baypol/servlet/fc?wacc_cmd=lkalogincommand.1&tlu=06101158&tlr=0900103030000_BTR&tle=1143047093828&tld=1143051053828&tlh=079628a

20060322-180807-XPOBVC01 (30)
□ 001
□ 002
□ 003
□ 004
□ 005
□ 006
□ 007
□ 008
□ 009
□ 010
□ 011
□ 012
□ 013
□ 014
□ 015
□ 016
□ 017
□ 018
□ 019
□ 020
□ 021
□ 022
□ 023
□ 024
□ 025

| | | | |
|---|---|---|---|
| Dienststelle: | PP Obb. SG IuK | | |
| Familienname: | Wust | StN: | 06101158 |
| Vorname: | Walter | Amtsbez.: | EPHK |
| Importdatum: | 22.03.2006 Uhrzeit: 18:10 | | |
| Medien-ID: | 20060322-180807-XPOBVC01 | | |
| Anzahl der Bilder: | 30 | | |

**Pic 1:**

Digital Images are managed by a Client-Server Application within criminal investigation processes. The best effect of the cost pressure in the market of peripheral devices may therefore be reached by defining lean processes for the device management that support the sometimes necessary change to new producers or different device types without significant investment of time or personnel. The result is the requirement for cost efficient life cycle management for a potentially very big “zoo” of devices and an efficient integration into the defined processes, especially the procurement and approval processes.

**The police authorities’ need for security is obviously high**, which leads to the fact that functions also need to undergo a “Negative Test”. Such a “Negative Test” challenges the function of one part of the component and checks it – in the ideal case under all circumstances. In this case the BIOS set-ups of some PCs showed an error: The “Plug and Play Mechanism” in the operating system and the operating system itself were “stronger” than the BIOS set-ups. Therefore, the lock of the USB interface, which had been defined by the BIOS, did not work in some cases and the user was able to access some devices - as a consequence the BIOS board tool did not pass the “Negative Test”.

Furthermore, the board tools BIOS and GPO do not allow the clearance of specific, named devices for users or user groups. In addition, those board tools also do not protect from interfaces or device classes that are unknown at the time of roll-out. Therefore, the system needs to be continuously updated.

The methods of ACL on single registry keys are already cancelled by the device drivers which, for example, immediately install a new registry key if they cannot read their own and look for a new location if they do not find writing authorization at a specific place.

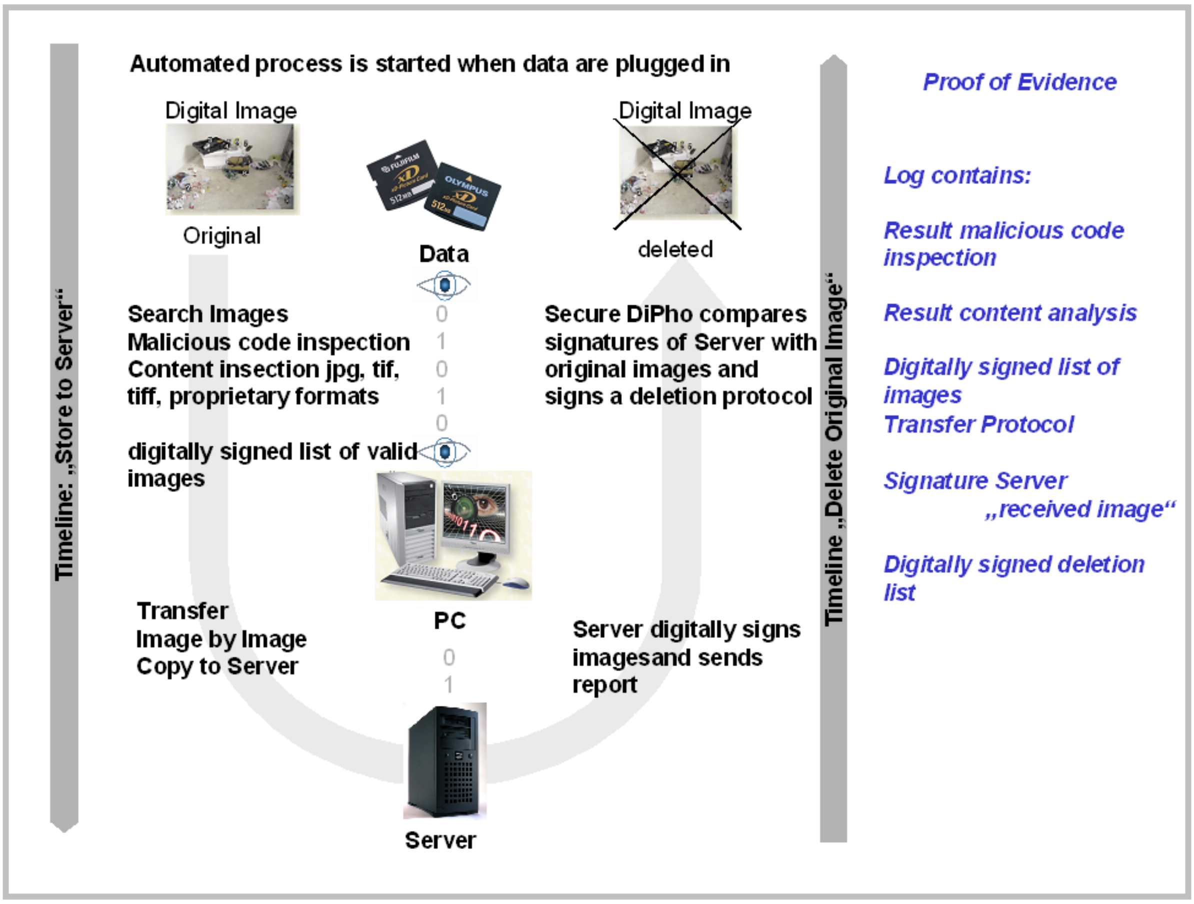
**After the analysis of all available board tools** it quickly became obvious that there is no appropriate board based solution due to missing flexibility and limited functionality. A brief market analysis – “Make or Buy” – clearly fell in

The Bavarian Police have defined that a photograph of scene of crime may **only be deleted** from the original data storage device if it has been **proven that an identical copy of the original photograph** has been **received by a dedicated server**. Technically, the photographs need to go through the following process:

1. Copying of the photographs from the original storage device into a quarantine zone and creation of integrity signatures for each photograph in the protocol
2. Checking the photographs for
   a. Viruses, e.g. they may not contain any so called “Malicious Code”
   b. Content, e.g. for semantic and syntactic correctness: Here, not only the known JPG EXIF and JFIF formats need to be considered but also producer typical raw formats that offer higher resolution and therefore make forensically detailed analyses possible.
3. After the positive check the photographs may be transferred to a server.
4. The server’s confirmation on a secure channel provides integrity signatures for each individual photograph.
5. The integrity signature is compared to the original photograph; the cancellation certificate will be created only if this content is correctly confirmed via a secure channel.
6. The photograph is deleted from the original data storage device and the cancellation protocol archived.
7. All individual steps and their results are lodged in a joint protocol and revision-secure log-file.

the favor of “Buy” because the products’ maturity did not justify an in-house-development and other locations were reporting significantly growing costs, even leading to cost explosion. For this reason, a call for tenders named “secure interfaces” was made at the end of 2004 looking for a tool which enables the secure management of individual devices and all interfaces. DeviceWatch from the Munich company itWatch GmbH was the winner of this call for tenders for the first half of 2005.

Parallel, a further challenge remained: A previously cleared device, e.g. a camera, could be misused by mistake or even on purpose.  Digital cameras are data storage devices with a file system which entails a multitude of risk scenarios. Principally, we distinguish the following scenarios when looking at misuse: (a) the *undesired export* – e.g. the writing onto a camera – and (b) *forbidden import* – the reading of forbidden material.


Timeline: „Store to Server“
Automated process is started when data are plugged in
Digital Image
Original
Data
Digital Image
deleted
0
1
0
1
0
Search Images
Malicious code inspection
Content insection jpg, tif, tiff, proprietary formats
digitally signed list of valid images
Secure DiPho compares signatures of Server with original images and signs a deletion protocol
PC
Transfer
Image by Image
Copy to Server
0
1
Server digitally signs imagesand sends report
Server
Timeline „Delete Original Image“
Proof of Evidence
Log contains:
Result malicious code inspection
Result content analysis
Digitally signed list of images
Transfer Protocol
Signature Server
„received image“
Digitally signed deletion list

**The solution mentioned** in the first scenario seems to be relatively easy because there is a flag under Windows XP that generally prevents writing to USB storage devices. Unfortunately this board tool is not sufficient either because it only works for USB – therefore does not consider integrated flash card readers – and furthermore, is very inconvenient for the daily use: Here, the administrator who is supposed to be entitled to write, has to change the flag every time and, most of all, the administrator must not forget to reset the system after using it. This manual action is not reasonable and furthermore, very error-prone. Additionally, when opening images from folders in which the images are saved, some standard applications make smaller changes to the directory and cancel the action with undefined errors when the file has been write protected. The final KO criteria is the integration in a secure process because it does not only distinguish between reading and writing but the deletion as an action may only be realized after the completion of some requirements.

**These requirements significantly exceed the distinction** between reading and writing. The investment protection does not allow proprietary software solutions which are tailored to one or individual camera producers or which need a software update for the clearance of a new camera type because the quality security process for the software is too expensive and too slow to meet the challenges of the fast moving device market. Besides the security, the requirements for ergonomics and cost-effective operation are significant. In the following, we will only outline some representative and significant characteristics:

1. **Ergonomics**
    a. The process needs to start automatically whenever a camera is connected through an external interface.
    b. The user must be continuously informed about the progress of the process.
    c. The user must be informed about the status and possible necessary activities by a final status report. Here, it is obviously important that the police are able to use its specific terms.

2. **Cost efficiency**
    a. Principally, a White List for cameras and flash data storage devices must be defined because privately purchased data storage devices may not be used.
    b. The approval of a new model for all users or single users must be possible during the daily business from a central position with minimal time effort (less than five minutes.) This also includes syntactic and semantic checks of the image contents. This must also be done on the individual raw data formats of the producers.
    c. The procurement process must be designed in a way that the user is immediately informed about the next steps when plugging in a forbidden camera. No additional phone calls must be necessary.
    d. The Security Policy life cycle must be reflected in a simple and revision secure way also in a quality cycle with test, validation and production environment without doubling the total infrastructure.
    e. A close integration into the service desk is desirable where ideally the service desk would be informed about “plug and play” errors in realtime.

**So consequently, a secure platform is necessary** that meets the following abstract requirements and at the same time is open for the integration of new expansions or special requests:

1. Detailed logging
2. Own processes should be able to be integrated, e.g. as plug-in with an “auto start“ function as the reaction to dedicated actions (i.e. camera is plugged in)
3. Standard processes are provided in the product (e.g. application for procurement, life cycle management of Security Policies)
4. Content filter provides content checks: semantic and syntactic elements must be able to be expanded from the customer side.

From an overall project view some soft decision factors are important besides the formerly stated hard factors. The decision for a new sustainable IT platform and the business processes based thereon are very complex and therefore are renewed on a five to ten year period. The decision for one software solution that safely and efficiently meets all project requirements is therefore not sufficient. It is obvious that the solutions for the project "DiPho" need to build the basis for further requirements of the e-government area for a secure and cost efficient service of interfaces and devices.

# The solution

**DeviceWatch** (www.DeviceWatch.de) is actively deployed on all PCs of the Bavarian Police – some 20,000. There are no open calls and there were no significant negative incidents during the validation or the roll-out period of the product. **DeviceWatch** solves all laid-out challenges and makes the central management of even enormous networks possible:

- The content filter - including a detailed customer-side expandable pattern matching (i.e. the syntactic and semantic control of the file contents) meets all actual and future requirements for the data exchange with external drivers
- All interfaces and peripheral devices – even those unknown today – can be centrally managed, a software update for improvements is not necessary
- Cost efficient integration into the processes "Procurement", "Application", "Approval", "Revision", "Life Cycle Management" and "Inventory"
- **DeviceWatch DEvCon** (Device Event Console) makes it possible to individually react to each de-centrally occurring device specific incident (e.g. "Plug and Play" errors, new driver, forbidden network card etc.) and therefore enables the immediate integration of custom made solutions
- The capability to integrate an individual customer plug-in meets the requirement for an open platform
- Inventory of peripheral devices without client installations through the **DeviceWatch** Scanner or the **DeviceWatch** Event Console **DEvCon**

The installed base and reference installations of **DeviceWatch** prove a high product maturity level and an inter-sectoral market penetration.
The necessary security for an investment for mission critical technologies is given by the clear product alignment together with the sustainable architecture.

**Find out in detail about our innovation and contact us at**

Info@itWatch.de or +49 (0) 89 / 620 30 100.

itWatch GmbH
Stresemannstraße 36
D-81547 Munich
www.itWatch.info

## Sources:

[Sch04] Peter Scholz: *Plug & Plague – Sicherheitsdefizite durch automatische Geräteerkennung.* In: KES – Zeitschrift für Informations-Sicherheit, Nummer 1, Seiten 6-9, SecuMedia-Verlags-GmbH, Ingelheim, Januar/Februar 2004.

[Sch05] Peter Scholz: *Unbekannte Schwachstellen in Hardware und Betriebssystemen.* Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005.