Kick-off meeting of the Project

Administration, PRF, Payments, Plan for the next 6 month ...

SPS 984520

Presenters:

Karol Nemoga, NATO Project Evaluator

Otokar Grošek, NPD

December 8, 2013

Project administration
Project Management Handbook

http://www.nato.int/cps/en/natolive/88.159.htm

- Mission Expenses
- Payment Request Forms
- Payments through NATO SfP funds
- Project Reporting

Mission Expenses

- Annex 2 a-c
- Missions are expected to be below 5000€, are paid from the Operational account
- Mission Expenses Form – MEF
  - After each mission/travel that will be paid a MEF has to be completed, signed by the traveler
  - Original tickets, receipts, ... are attached to the MEF, kept by PCodirector
- Travel expenses – air or train tickets, and taxi from airport/train station are reimbused (private car – 1st class train ticket)
- NATO Per Diems Rate – 50 EUR per day (see below)

Training and Travel Missions

- Scientists in the Project involved are sent to conferences, meetings (different places, rather than group in one place).
- Advantageous situation – Project meeting coincides with the conference, sevaral people from one institute may participate.
- All missions **must** be approved by **NPD/SK** prior the mission...
- If the mission is outside EAPC (The Euro-Atlantic Partnership Countries), or more than 30 days training – explicit approval from **SfP Office** prior the mission is **required.**

Knowledge Transfer

- Regular project meetings with all key participant (end users) are **necessary.**
- SfP Office can send a staff member or consultant or steering committee member to the meeting – therefore date, place and agenda should be **announced in advance.**
- Participating of End-users from the beginning is recommended.
- Following the meeting a brief report is sent to the SfP Office (NPD).
- Meeting should take place in NPC (Israel).
- Advisors and Experts can be engaged (max 10 days per year). Necessary travel and living expenses are reimbursed.

Annex 2a, p. 21

Regulations and Accounting fro Mission Expenses

- All mission expenses are used in accordance with the Project Budget, and rules below
- Mission expenses may be paid with VAT
- Transportation
  - Air ticket (**not bussines**), 1st class train, economy in fast train,
  - When Apex, pex or excursion rates are applied – resulting to longer stay, living expenses are possible to reimburse
  - Private car – 1st class train
  - Car rental – exceptional

Annex 2a, p. 21

Regulations and Accounting fro Mission Expenses

- Accomodation, living and additional expenses
  - Real expenses according to the hotel bill (bed and breakfest)
- Living expenses
  - 50 EUR per day – should be reduced if host is paying for all meals
- Additional expenses
  - conference fee, taxis from airport, ... upon receipts only

Annex 2a, p. 21

Regulations and Accounting fro Mission Expenses

- Travel Advance
  - Not more than 75 % of estimated expenses – responsibility of project codirector
- Final Accounting
  - Reimbursement must be fully documented
  - Completed MEF signed by traveler, (MEF – Annex 2b, p.22, Example Annex 2c, p.23)
  - Original tickets, bills, receipts, …

PRF - Payment Request Form

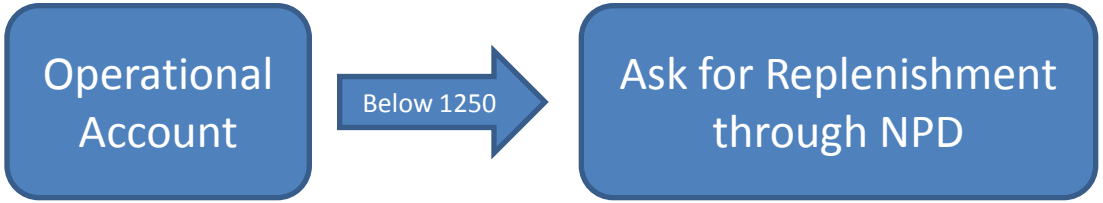
- PRF is like a bank transfer form: needed for each money transfer from the grant to any outside NATO account. p.2, Annex 1a, 1b
- Back up documents should be collected with each participant, NPD is collecting originals of PRFs, giving seq. numbers, signature, and will send them to SfP PO. p. 7
- Advance for a specific item: If Op. Acc. does not cover the full price – request through PRF for the difference, or whole amount.

PRF - Payment Request Form

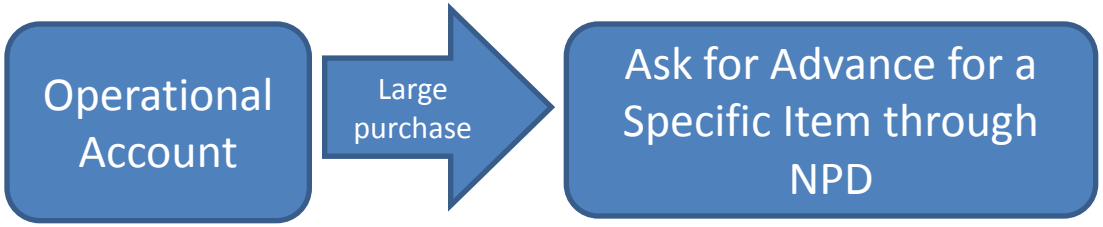
- Cash withdrawal from Oper. Account should be an exception for specific use only. p. 7
- To pay VAT is not allowed except of travel expenses.
- Procurements of equipment, consumables, spare parts... should be from vendors or manufactures located in NATO or Partner country. The exception – SfP Program Director... p. 10

PRF - Payment Request Form

- Replenishment of Op. Acc.: attach table listing the items paid from Op. Acc. from the last Replenishment. p. 8-9, Annex 1d
- For values less than 5000€



- For values less than 5000€ but a large purchase



PRF - Payment Request Form

- For values more than 5000€ : will be paid by NATO directly to the vendor 50% in advance, and 50% upon delivery see sec. 4 p. 9
- For values more than 12500€ : will be paid by NATO directly to the vendor 50% in advance, 40% upon delivery and 10% upon successful instalation – oscilloscope only?

  In this case a special paperwork is required for each step. see sec. 4 p. 9

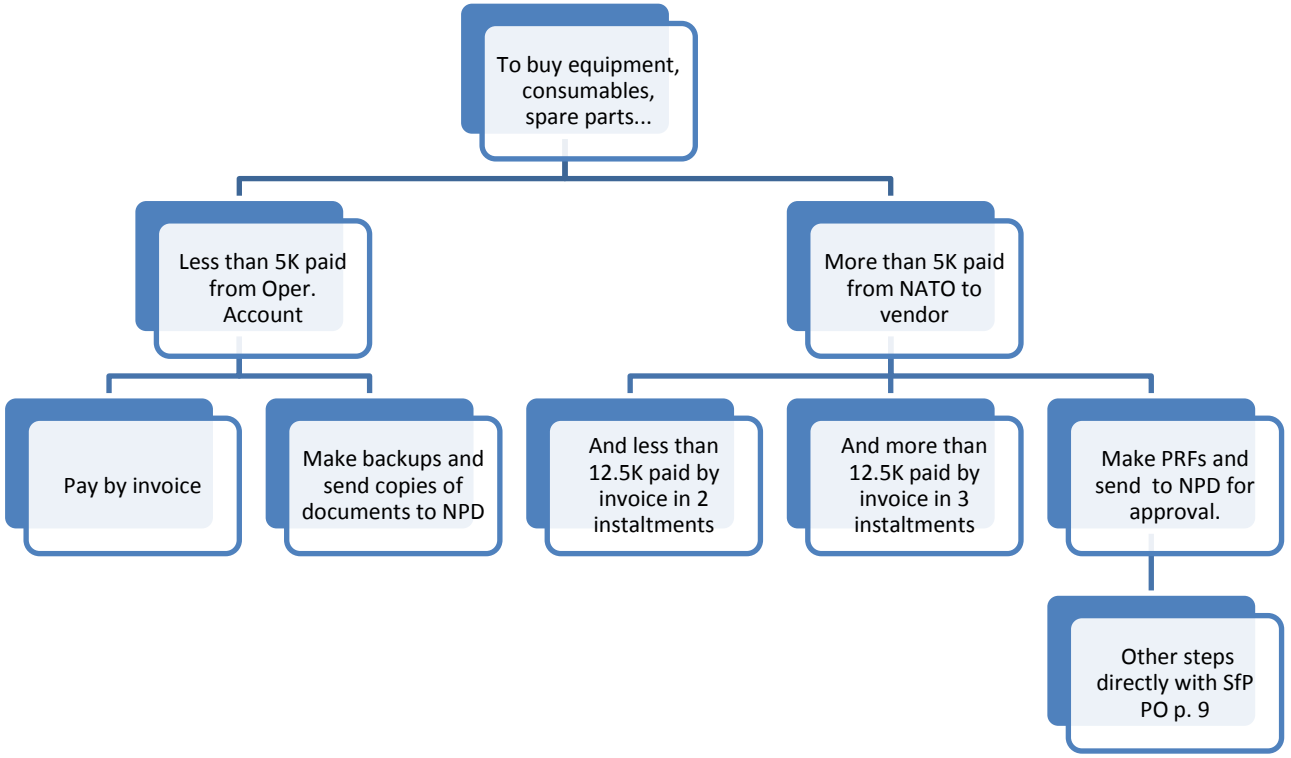
Major budget items

Item	Estimated price	Cofunding	Purpose
Oscilloscope (4GHz bandwidth, 4 channels, 125Ms/ch),	47000	7990	Measurement of emanations from the implementation.
Oscilloscope probes (3.5GHz differential and single-ended)	10000	1700	Probes capturing physical emanations and representing them as analog electric signals.
Spectrum analyzer (4GHz, wideband IF output)	6250	1060	Signal analysis and conditioning.
Antennas, Low-noise amplifier	7000	1190	Signal reception.
Motorized XYZ table with micron precision	10000	1700	Location of measured points.
Smartcard, PC and FPGA test targets	10000	1700	Hardware analysis.
Lab furniture for equipment, installation and peripherals	8250	1400	Physical setup for operation.
Altera DK-DEV-4SE530N development kit, 2 sets	11000	2200	Implementation of FPGA design.
Quartus II license and a high-end PC, 2 sets	7000	1400	FPGA circuit design.
High-end PC with at least 128 GB RAM (like DELL PowerEdge T610)	8000		A powerful PC for cryptanalysis.
Magma computer algebra system	5000		Allows fast finite field computations.

Payments through NATO SfP funds

- Changes in the budget less than 5000€ - approval by NPD. If more, an approval by the SfP Program Director is needed. p. 5
- Even if the value is less than 5K the Co-Director may request this through a PRF... p. 7
- In all cases when the purchased item was paid from NATO directly, when received the original invoice, it must be sent to SfP Programme Office with indication of the current PRF document. p. 8

How to pay when PRF paperwork is finished



Payments through NATO SfP funds

- For PRFs there are two ways:

1. *If the original back-up documents are required to be kept by Institute of Co-Director.* Mark the original back-up docs with "Submitted to NATO for payment" - take a copy - send the copy and original PRF signed by Co-Director to the NPD.

Payments through NATO SfP funds

2. *If Institute of Co-Director does not require to keep originals, e.g. when it is paid by Brussels.*
Mark the original back-up docs with "Submitted to NATO for payment" - take a copy - send the original back-up docs and original PRF signed by Co-Director to the NPD.

Payments through NATO SfP funds

In both cases the NPD counter-signs the original PRF and sends all docs to the SPS Projects Office. If the NPD wishes to make copies for his file then he may do so.

When submitting by e-mail, please scan the originals.

Competitive binding, sec. 4.2

- For purchases of a value below 12,5K telephone inquiries may be sufficient but not compulsory...
- For purchases of a value over 12,5K CB is performed by Co-Director – to establish a level of assurance that the item will meet the Project´s requirements...
- The NPD and SfP Program Office final approval for items more than 5000€ is required.

Project Reporting
Section 8, p. 14

- NPD, NCC and PPD are jointly responsible for reporting (sec. 1, responsibilities of codirectors, p. 4).
  - Codirectors are responsible to support NPD with all information needed for the preparation and timely submission of reports to the SfP Office.
  - In the case of major budget changes (>5000), revised budget tables will be included in the financial part of Progress report.

Project Reporting
Section 8, p. 14

- Dissemination of the results generated by the project
  - Periodic seminars, conferences papers, posters, Journal papers... (should be sent to the SfP Office through NPD).
  - Add everything to the web-page of the project.
- All documents should mention the SfP. Recommended text:

  This research is sponsored by NATO's Public Diplomacy Division in the framework of "Science for Peace".
- Visibility of the project
  - WEB site, from the beginning of the project (hyperlink from NATO WEB will be established), user names, passwords...
- All related documents and actions should be included in 6 months reports.

Progress Report
Annex 3a, p. 24

- Structure
- Six pages – precisely defined description of the project
- Five separate Chapters, three colors paper used by NPD (white, rose, rose, yellow, white)

Progress Report
a) Technical Progress, p. 25

- Accomplishments achieved (acc. Aproved Project Plan)
- Actions taken
- Milestones for the next six months
- Involvement of young scientists
- Major travel
- Visits of NATO assigned officers
- Visibility of the project
- Difficulties, if any
- Changes, if any, in the Project Personnel – right now...
- Changes, if any, in the Project Plan

Progress Report
b) Financial Status, p. 25

- Set of tables (Annex 4a, 4b, 4c) completed by NPD
- Budget table, Annex 4a, with actual expenditures, forecast expenditures (next six monts, to the end of project)
- Budget summary table, Annex 4b, (per codirector and budget items)
  - Aproved budget,
  - Current cost outlook,
  - Actual expenditures,
  - Forecast expenditures
- SfP National Contribution Table, Annex 4c

Progress Report
c), d), e) Parts, p. 25

- c) Equipment Inventory Records, Annex 5, p.31
- d) Criteria for Success Table, Annex 6. p. 32
- e) Two page Summary Report, annex 7, p. 33-34
  - Description of the project
  - Abstract of research
  - Major objectives
  - Overview of achievment since the start
  - Milestones in the next 6 months
  - Implementations of results

- Final Report, Annex 8, p. 35-36, up to 54 pages

Novelty in the project

- Project emphasis on **cryptographic constructions building on error-correcting codes and lattices.**

- Experimental work with **actual measurements for different implementation platforms**, and **more thorough theoretical analysis** of involved computations are urgently needed.

- **Insight into plausible hardware modifications** to protect sensitive (key) material adequately .

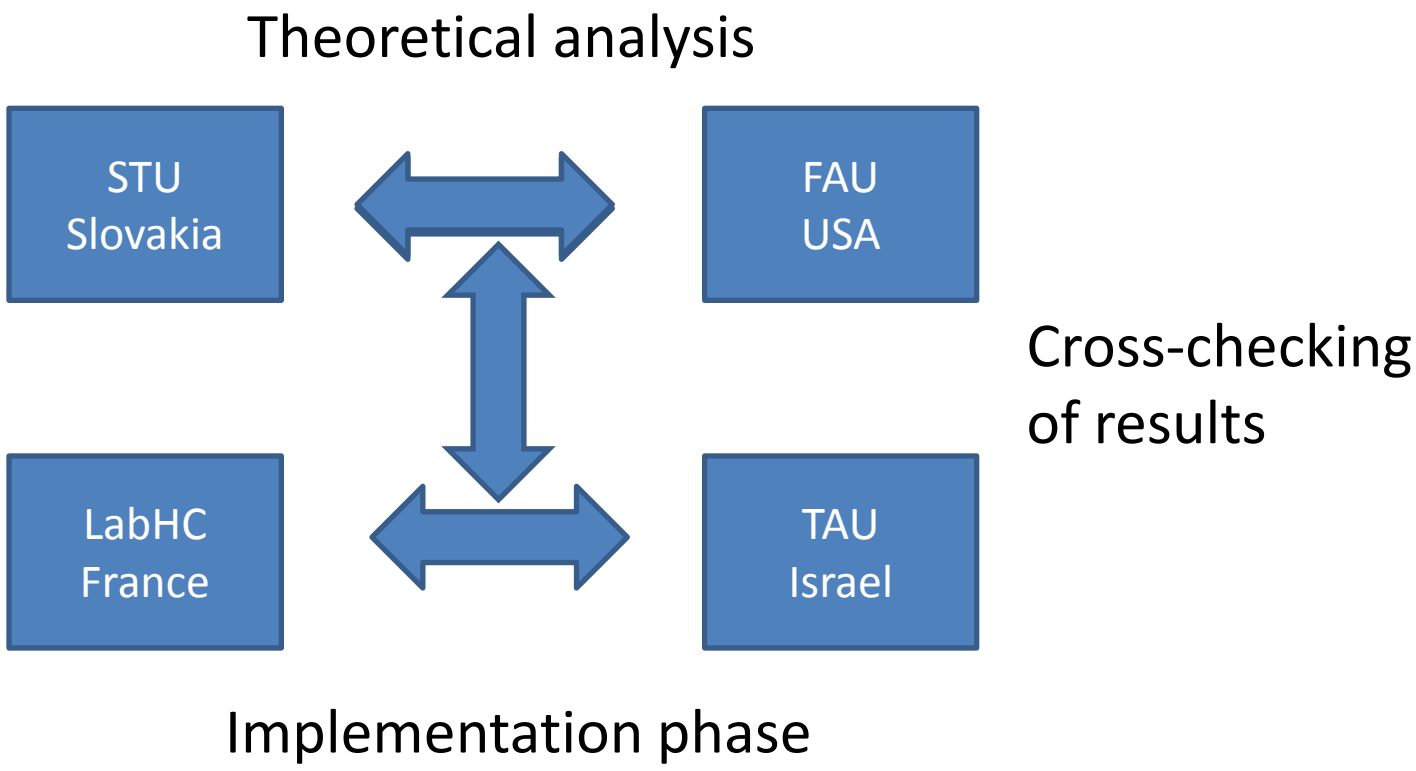
Deliverables and milestones

MILESTONE	TIME	DELIVERABLE
1. Project setup, equipm. ordering, Kick-off meeting.	1 – 6 month, 1st year	Project WEB site
2. Software implement. and test vectors.	1 – 9 month, 1st year	Test vectors of functions for hardware implementat.
3. Selected hardware functions (in VHDL)	7– 12/ 1-3 month, 1st/2nd year	The code and executable files for selected algorithm
4. Fully operational setup to measure and process.	7– 12/ 1-6 month, 1st/2nd year	The code and executable software to measure.
5. Capability to carry out side-channel attacks in 2.	10– 12/ 1-9 month, 1st/2nd year	Software to perform side-channel attacks.
6. Mounting efficient side-channel attacks.	10– 12/ 1-6 month, 2nd/3rd year	Extracting secret data and recommended parameters.
7. Dissemination of results.	4– 12/ 3rd year	Results available to End-users and NATO.

Criteria for success

Aggregated Criterion	%
1. Project set up and realization of kick-off meeting.	5%
2. Software implement. and test vectors.	18%
3. Selected hardware functions (in VHDL)	18%
4. Fully operational setup to measure and process.	8%
5. Capability to carry out side-channel attacks in 2.	10%
6. Mounting efficient side-channel attacks.	21%
7. Dissemination of results including training of Israeli students.	20%

Communications plan



Communications plan - continued

No strict separation of theoretical and experimental work, but

- Main share of implementation: Tel Aviv University & Jean Monnet University.
- Main share of theoretical analysis: partners in Slovakia and the U.S.

- Complementary measurement facilities in France and Israel: parallel research on different schemes or platforms.

- Partners in Slovakia and the U.S.: established track record in the theoretical analysis of post-quantum schemes

Experts from other NATO countries

Name	Affiliation	Role
Tim Güneysu	Assistant Professor and head of the Secure Hardware group at Ruhr University Bochum, Germany	FPGA implementations
Peter Horák	Professor at the Interdisciplinary Arts and Sciences, University of Washington, Tacoma, USA	Solutions of coding and combinatorial problems
Thomas Eisenbarth	Assistant Professor at the Department of Electrical and Computer Engineering Worcester Polytechnic Institute, MA, USA	Efficient and secure implementation of cryptographic algorithms
Tal Malkin	Associate professor of Computer Science at Columbia University, NY, USA	Leakage-resilient and tamper-resilient implementations of cryptographic schemes.
David Naccache	Professor at Université Paris II, Panthéon-Assas, France	Exploring countermeasures against side-channel attacks.
Francois-Xavier Standaert	Professor at the UCL, Institute of Information and Communication Technologies, Electronics and Applied Mathematics, Belgium	Side-channel analysis.

End-users and their contribution

- **National Security Authority of SR** 

  Will utilize all theoretical & practical results gained by this team. If necessary will allow the team to utilize some laboratory equipments.

- **STMicroelectronics, FR** 

  Can provide feedback and challenge the research results, giving an industrial standpoint, provided the broad range of applicative markets served by STMicroelectronics.

- **First Data Corporation, USA** 

  Will contribute to project development by providing harvested raw data that will be used to detect possible side channel attacks & by providing inputs to support new applications & services based on the gained information. Helps with promoting project results & solutions in regulatory and standardization bodies, offers support in business case analysis, if necessary.

Dissemination of results

- Public conferences organized by the project teams
- Presentations of results in international conferences, as well as domestic workshops
- Publications in international scientific journals
- Cooperation with the broader research community, including NATO experts from other countries
- Dissemination through a web site, appearance in popular media and press

Questions

- How and when to invite Experts...
- Plan of Training.
- Next meeting in St. Etienne ? Invitation of End-users.
- How flexibile will be HW implementation (e.g. if a different code is selected, different algos will be invented,...).

Questions

- Is it necessary to generate polynomial g for Goppa code randomly, or can it be fixed ?
- Are there any interoperability standards for key storage, padding, etc. for McEliece system (like X.509)?
- Possibility to use Lee-codes ?

Thank you for your attention!