



**secunet Security Networks AG**

**Решение за криптиране на  
информацията на държавните власти**

# СЕКУНЕТ – МРЕЖОВА СИГУРНОСТ

## SINA – ОБЩ ПРЕГЛЕД

Sofia, 10.06.2014



## Съдържание

1. Корпоративен преглед
2. Препратки и препоръки
3. Продукти
4. Приложение в Министерството на външните работи на Германия
5. Приложение в Министерството на отбраната на Германия
6. Приложение в Министерството на вътрешните работи на Германия
7. Приложение в разузнаването на Германия

## 1

## Корпоративен преглед

- Водеща германска компания с отлични решения за защита на IT мрежи за класифицирана информация
- Изключителен партньор на German Federal Office for Information Security (BSI) /Германската федерална служба за информационна сигурност/
- Изключително висок опит в обслужването на държавни власти и международни организации

## 2

## Клиенти - Потребители

Развърнато и използвано в 8 европейски страни като национални стандарти

- Министерството на външните работи на Германия – мрежа с всички посолства по света-300 локаций с централно менажиране/управление
- Германските въоръжени сили и Министерството на отбраната - най-големият клиент с 14,000 потребителя и техните военни мисии
- Германска гранична полиция - Сложен комплекс и комбинации от 400 потребителя за граничен контрол
- Офиса на Министерството на отбраната в НАТО – Обмен на класифицирана информация между Националния и НАТО офиси
- Европейска комисия  
Мрежа между 27 нации и Европейската централа

## 2

## Клиенти - Потребители

Развърнато и използвано в 8 европейски страни като национални стандарти

- NATO Главна квартира  
Стационарните и мобилни щабове на Силите за отговор на НАТО
- Европейски въоръжени сили  
Многонационални сили за бързо реагиране
- sTESTA – Европейски граничен контрол  
Защита на границите на Европейския съюз
- IVBB – Федерални комуникации Бон-Берлин, свързващи министерства в двата града в една мрежа

## 3

## Продукти – SINA сигурност на комуникациите



- SINA Vox - IPSEC VPN, акредитирано за ниво “Строго секретно” в Германия, Секретно в НАТО и ЕС

SDIP ниво A / Zone 0 - гарантирано (tempest доказани хардуерни решения)



- SINA L2 - двупластов – основа на криптирането, осигуряваща до 10 Gbps напълно сигурен поток през IPsec тунела



- SINA One Way Gateway  
Трансфер на данни на физически разделени мрежи в общ поток

## 3

## Продукти – SINA сигурност на комуникациите



- SINA Thin Client  
Терминал сървър - потребител, акредитиран до ниво “Строго секретно”

SDIP ниво A / Zone 0 - гарантирано (tempest доказани хардуерни решения)



- SINA Virtual Workstation  
Мобилно решение за бизнес компютри (Lenovo) и специален хардуер (Roda, Toshiba)



## 3

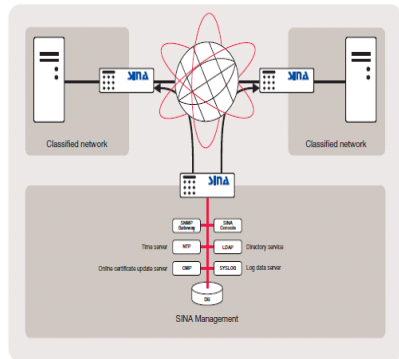
## Продукти – SINA сигурност на комуникациите



- SINA Mobile Disk  
Защитаващ класифицираната информация в ултра мобилен USB хард диск
- Отлично хардуерно криптиране
- Тайният (PIN) трябва да се въведе директно на устройството

## 3

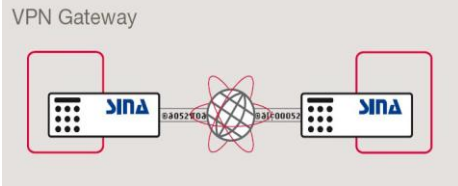
## Продукти – SINA Management /управление/



- SINA Management управлява всички SINA компоненти и е ключов компонент за контрол на управляваният комплекс и мрежите за защитена информация.
- Технологията дава на администраторите пълен контрол върху действията на допуснатите потребители да инсталират и използват личните си крипто устройства в отдалечените локации.
- SINA VoX, L2, OWG и Thin Client нямат информация във себе си и трябва да бъдат управлявани централно.

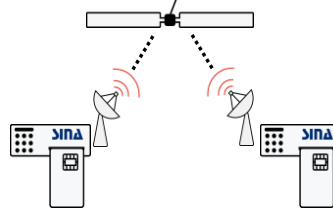
# 3

## SINA – приложение на продуктите

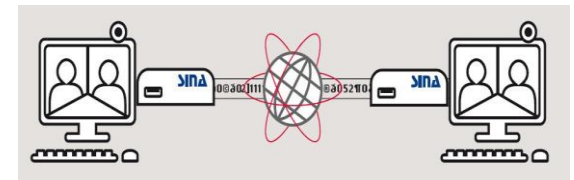


### Network 2 Network

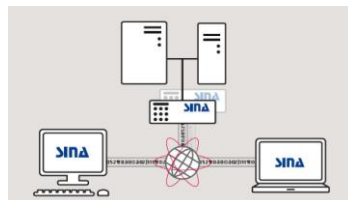
### Secure Satellite Connect



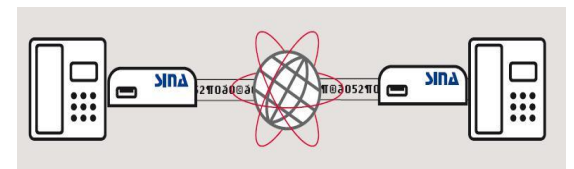
### Secure Video Conferencing



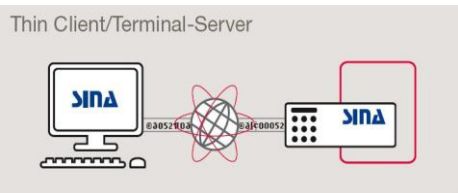
### Hot Stand-by



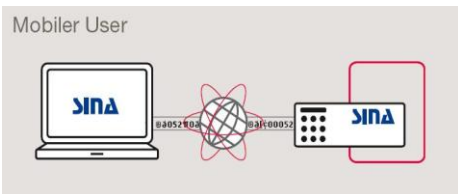
### Secure Voice-Over-IP



### ThinClient 2 Terminal Server



### Mobile User 2 Office LAN



## 4

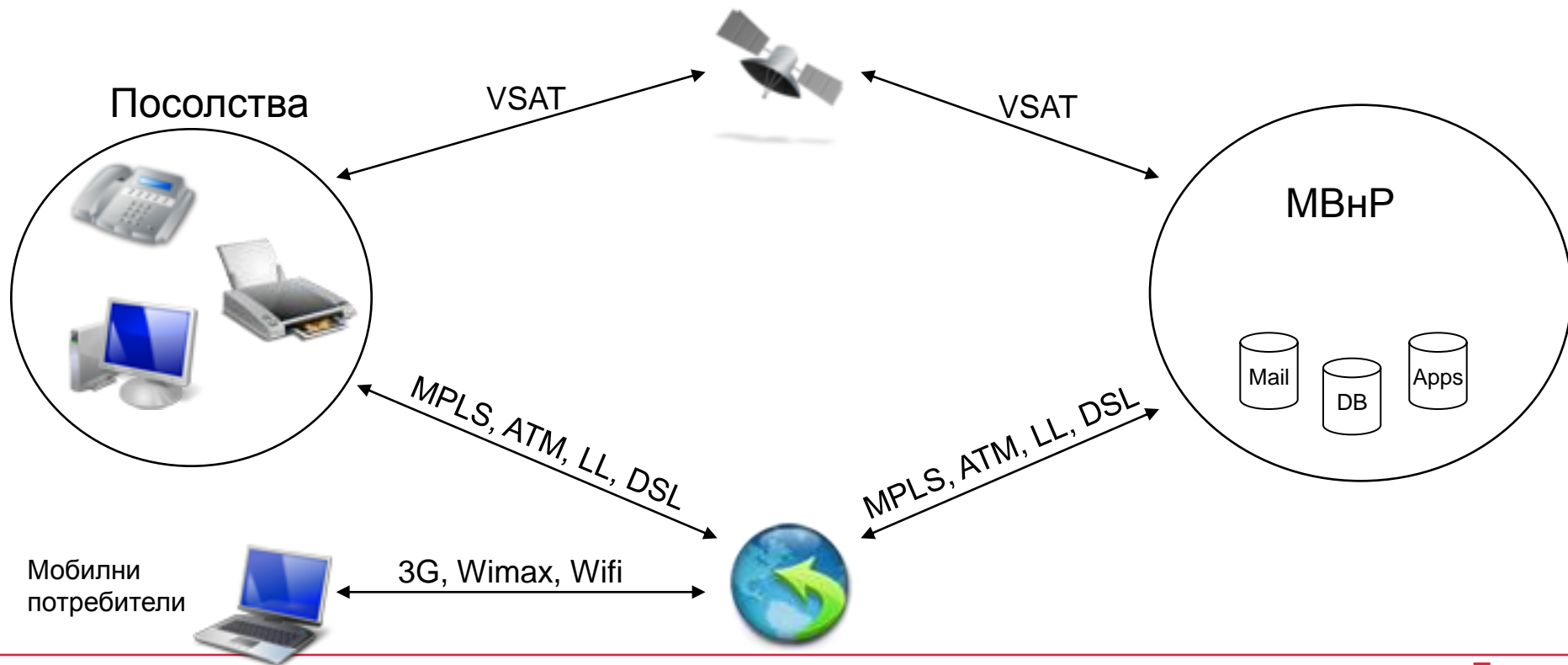
## Приложение: Министерство на Външните работи

Мрежа с  
посолствата  
в целият  
свят

- Сигурност на изградени мрежи за информация в целият свят
- Използуване на общодостъпни комуникационни линии
- Осигурява устойчива работа в не особено приятелска среда на разпространение, и при загуби на информация при преноса
- Осигурява и поддържа голямо изобилие от възможности за мрежово свързване
- Управлява всички устройства централно
- Позволява лесна експлоатация от потребителите (plug and play)
- Осигурява незагубване на информация в извънредни случаи

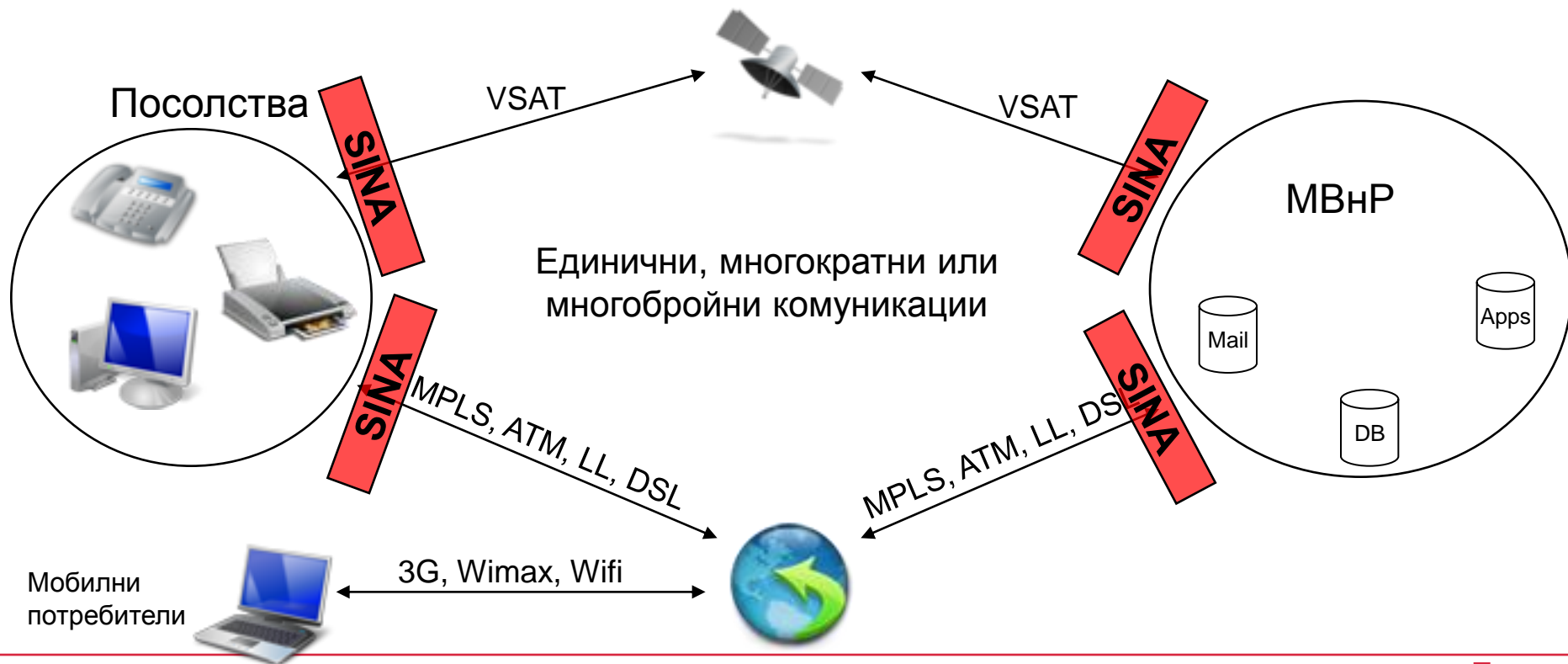
# 4

## Приложение: Министерство на Външните работи



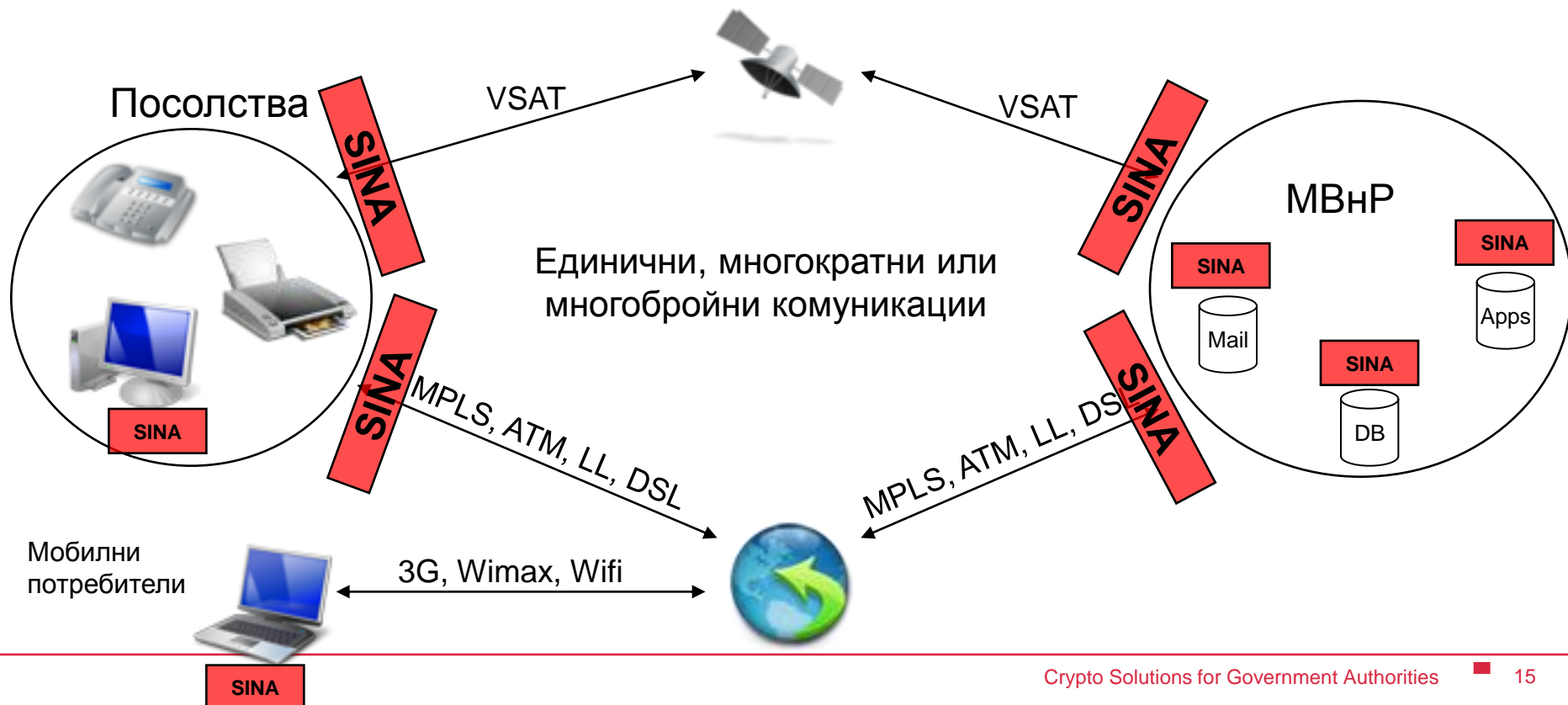
# 4

## Приложение: Министерство на Външните работи



# 4

## Приложение: Министерство на Външните работи



## 5

**Приложение: Министерство на отбраната**

- Изградени мрежи за защитена и класифицирана информация във враждебна среда
- Използуване на комуникационни линии в бойно поле
- Осигурява устойчива работа в не особено приятелска среда на разпространение, и при загуби на информация при преноса
- Осигурява и поддържа голямо изобилие от възможности за мрежово свързване
- Поддържа работа с мобилни устройства
- Разрешава достъп до информация с различни нива на класификация

Централизирано  
управление  
на мрежите



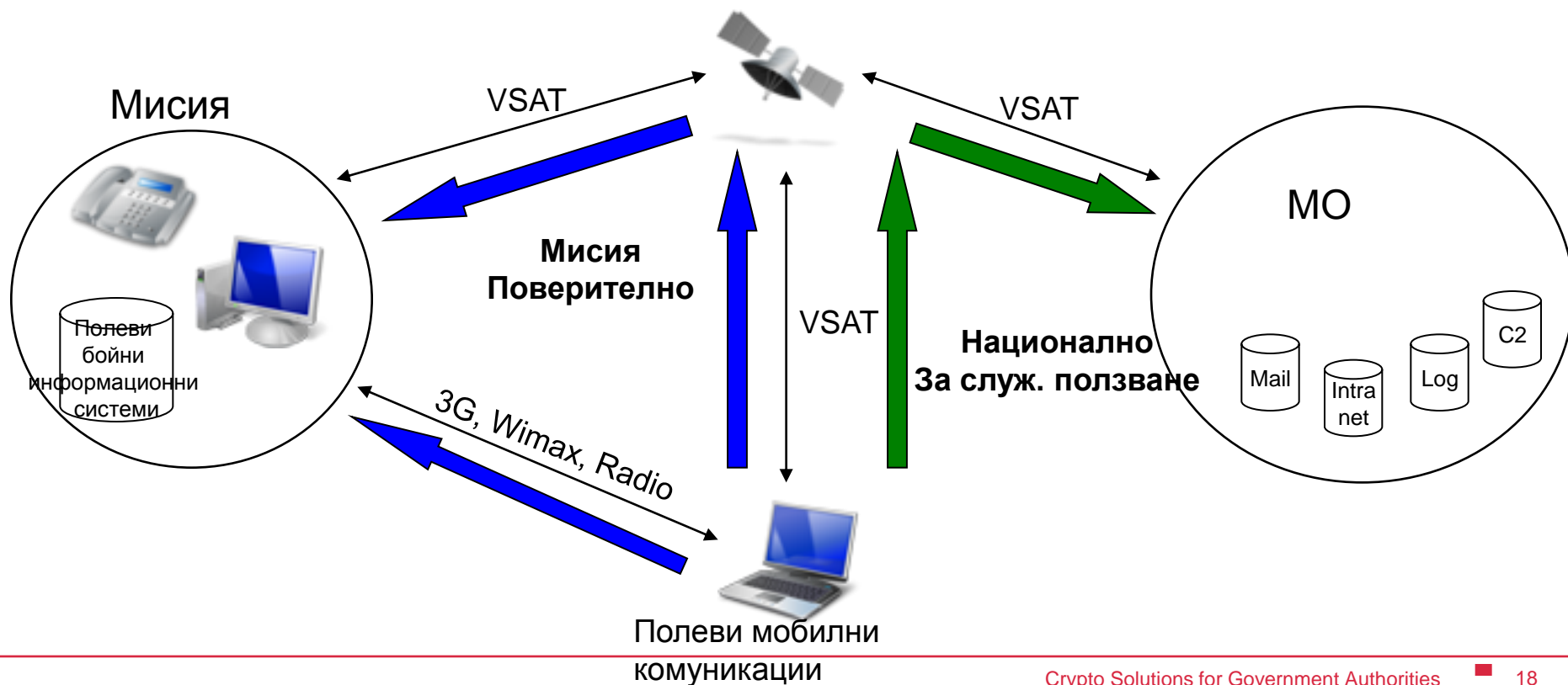
# 5

## Приложение: Министерство на отбраната



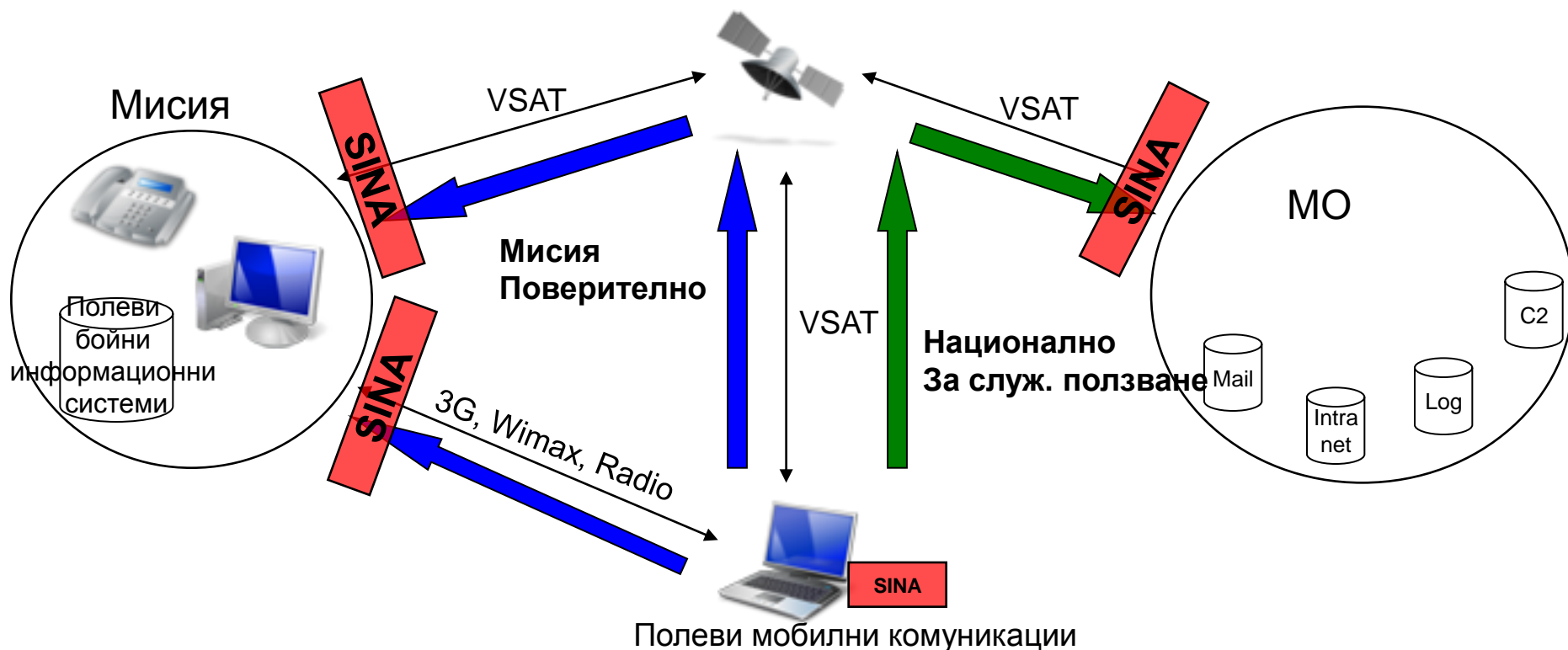
# 5

## Приложение: Министерство на отбраната



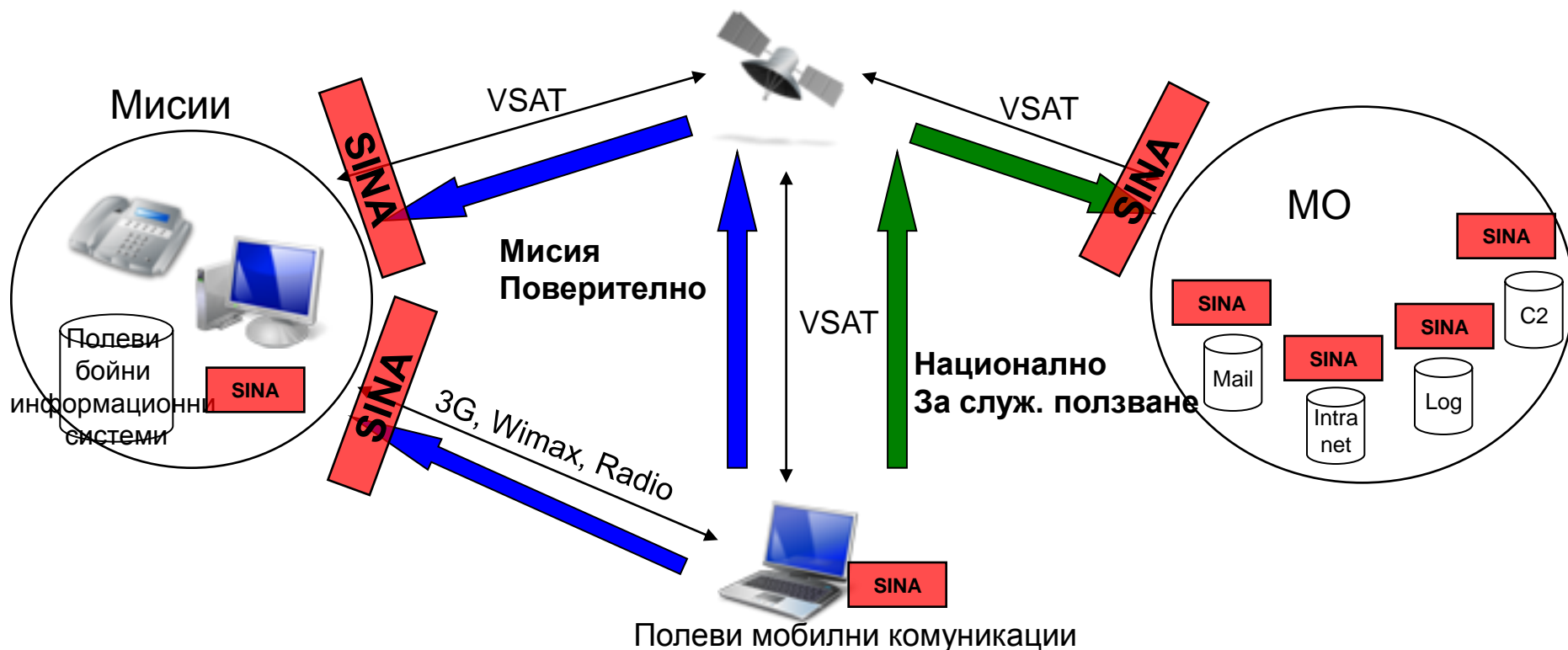
# 5

## Приложение: Министерство на отбраната



# 5

## Приложение: Министерство на отбраната



## 6

## Приложение: Министерство на вътрешните работи

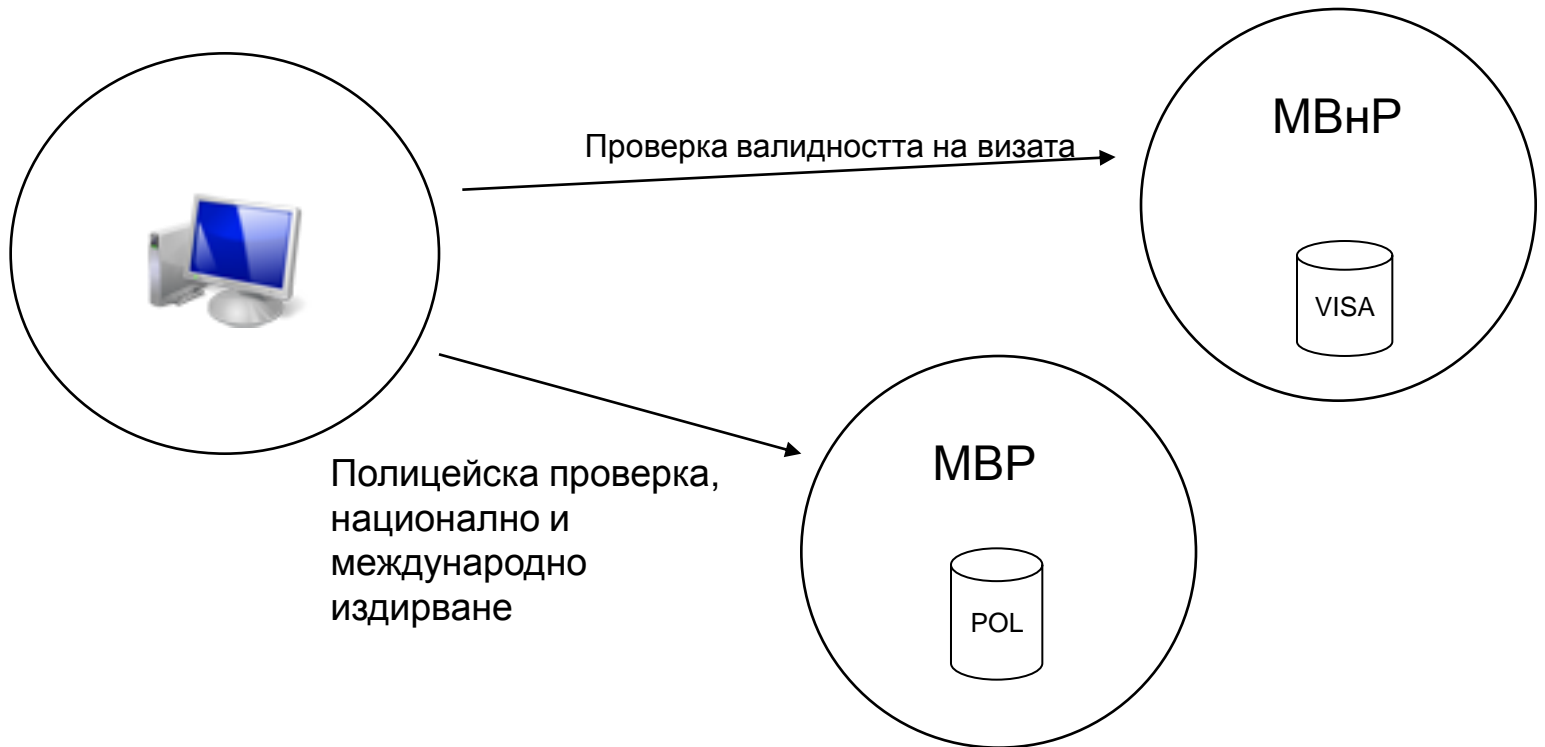
Граничен и имиграционен контрол

- Изградени бързи и благонадеждни мрежи
- Разрешава достъп до централизирани приложения и ресурси
- Критични среди, неразрешаващи времеви нарушения (летищни сценарии)
- Разрешава достъп до информация с различни нива на класификация

# 6

## Приложение: Министерство на вътрешните работи

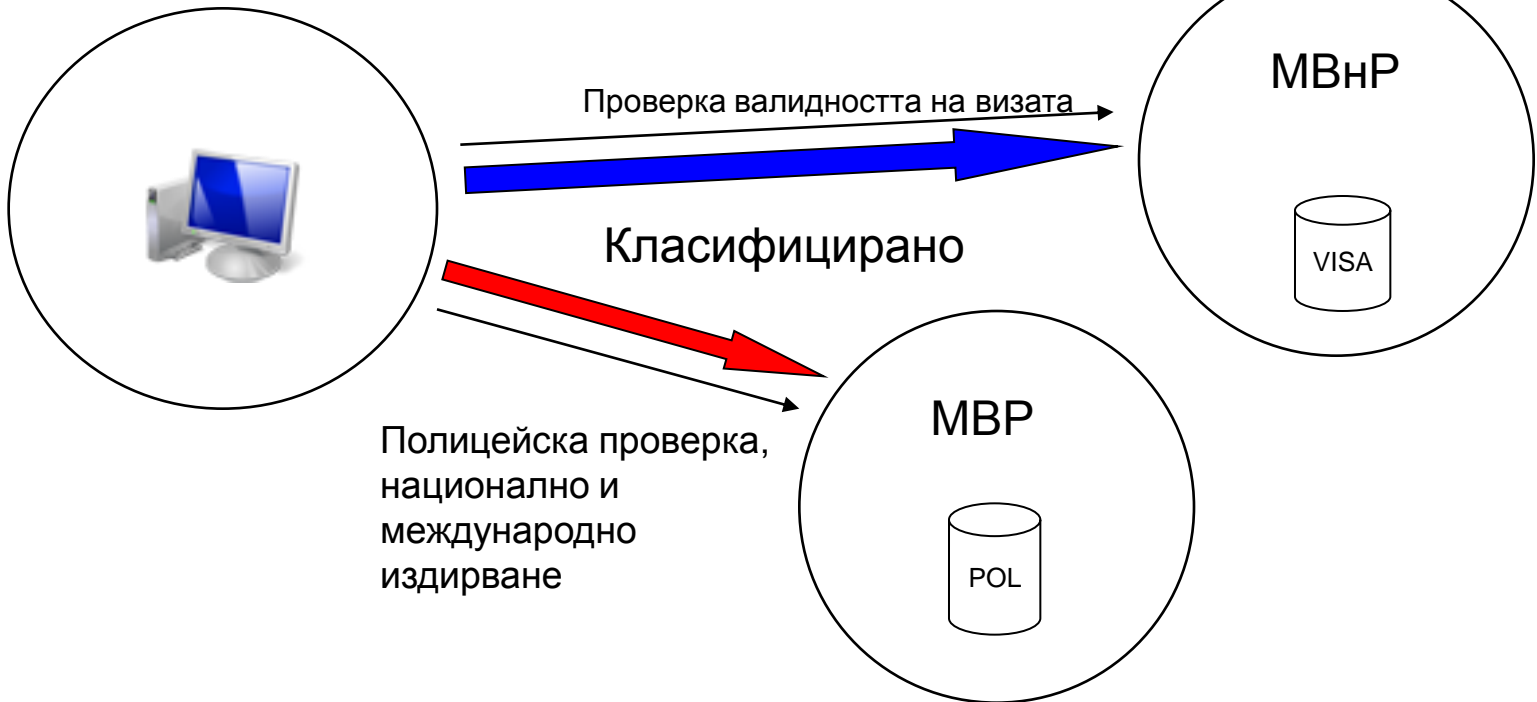
Гранична  
полицейска  
станция



# 6

## Приложение: Министерство на вътрешните работи

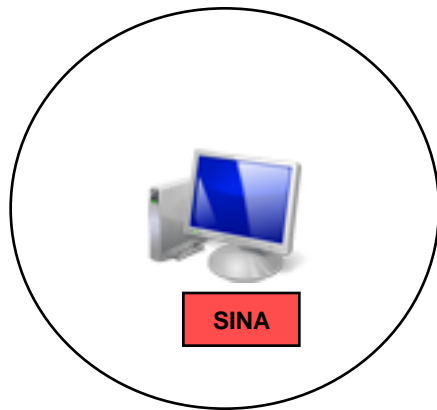
Гранична  
полицейска  
станция



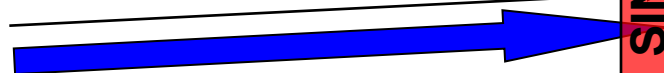
# 6

## Приложение: Министерство на вътрешните работи

Гранична полицейска станция



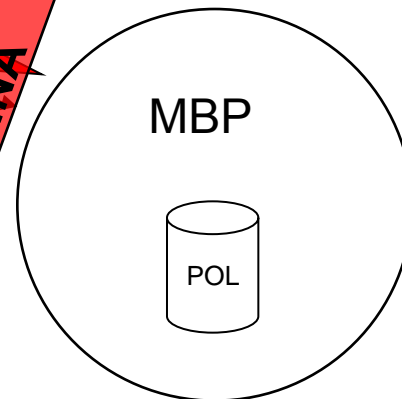
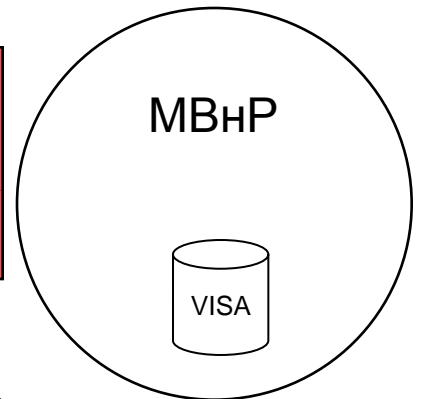
Проверка валидността на визата



Класифицирано



Полицейска проверка, национално и международно издирване





# 7

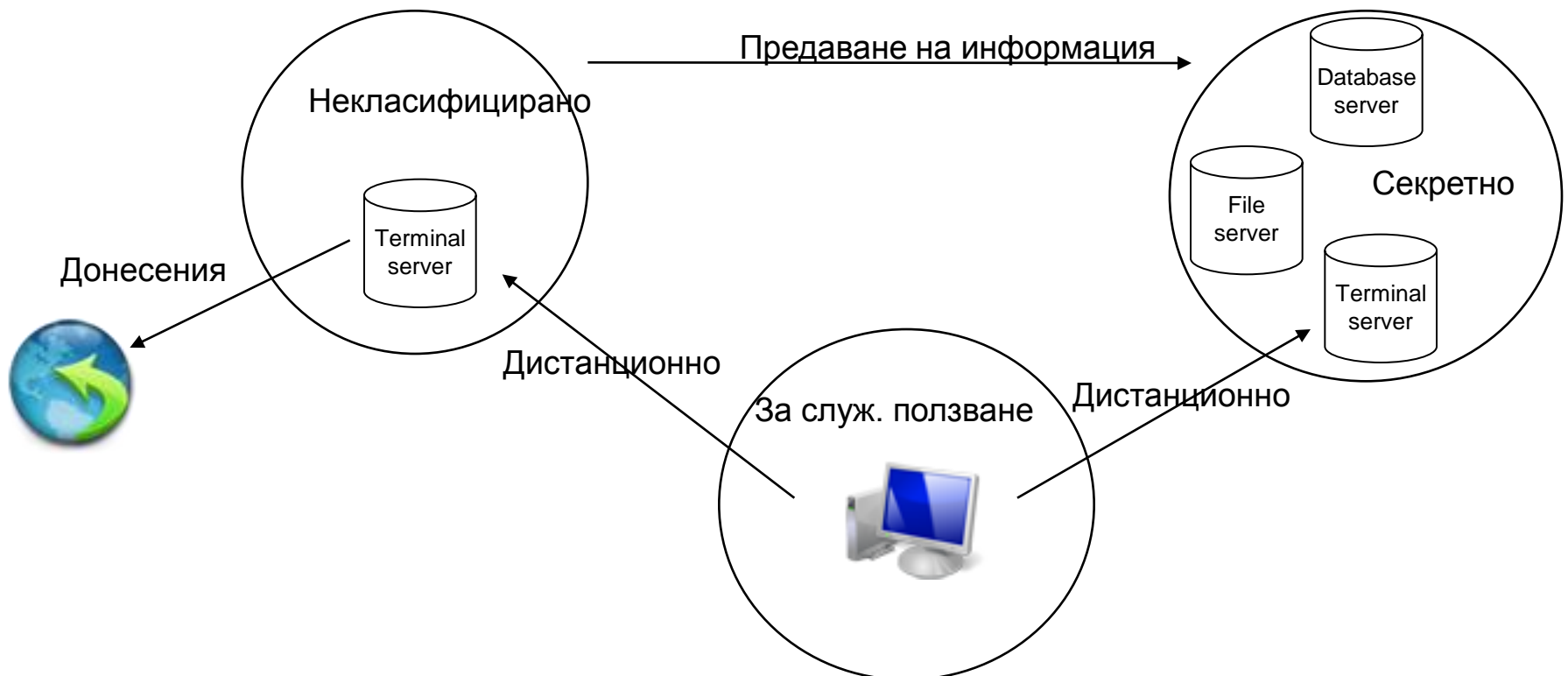
## Приложение: Разузнаване

Законно  
радиозаглушаване

- Осигурява висока сигурност на мрежово разделяне
- Осигурява достъп до ресурси с различни нива на класификация
- Използване на неklasифицирани мрежи за обратно изпращане на информация и донесения
- Трансфер на информация от неklasифицирани в класифицирани мрежи, нямащи физическа връзка

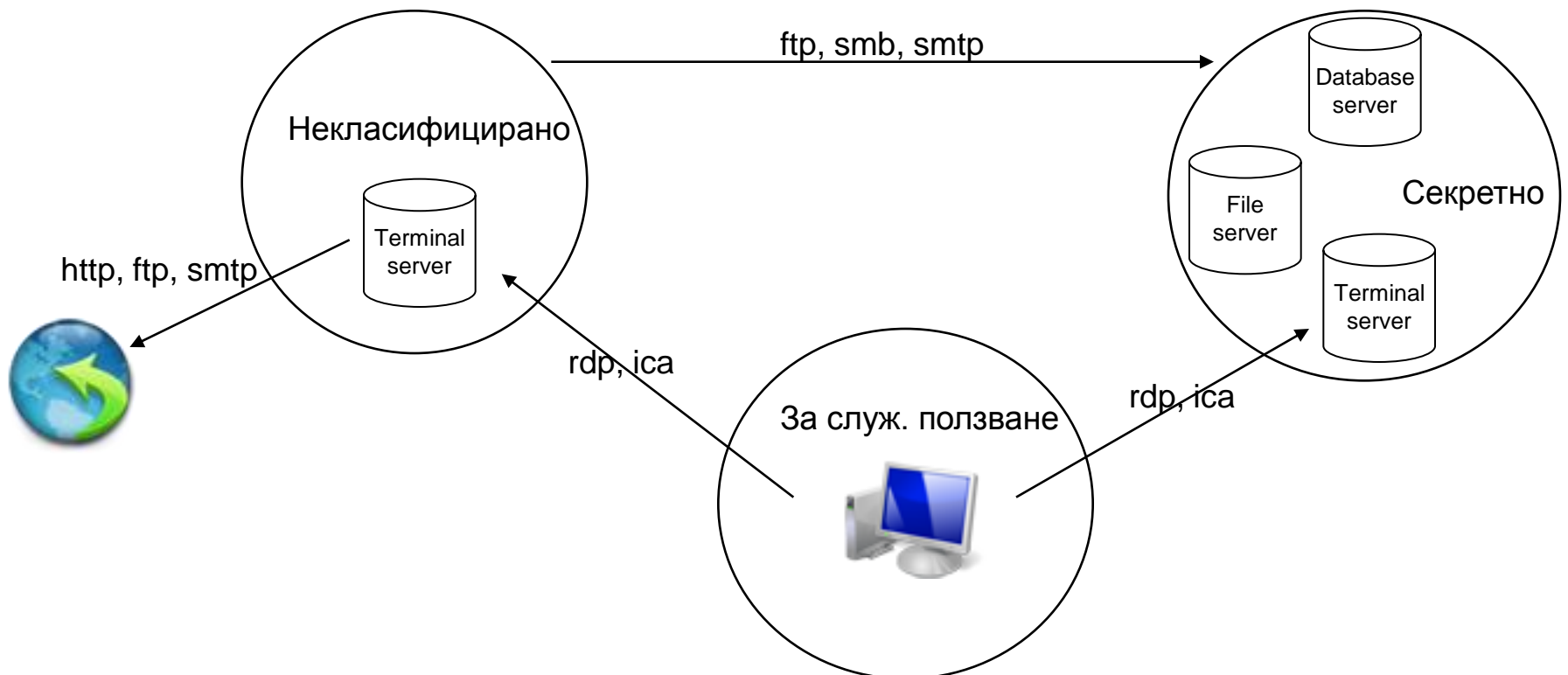
# 7

## Приложение: Разузнаване



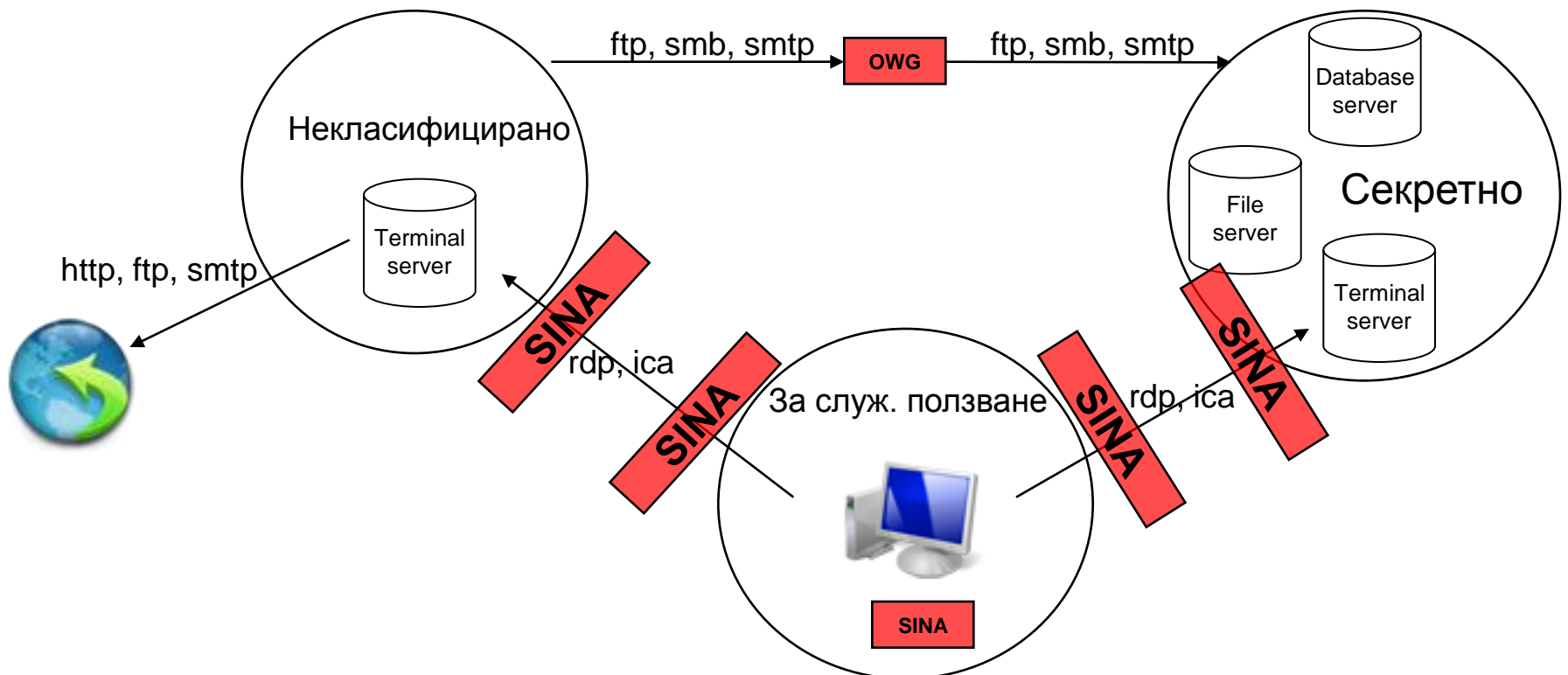
# 7

## Приложение: Разузнаване



# 7

## Приложение: Разузнаване



# 8

## Приложение: Изграждане при различни нива на класификация

Защита на информацията по нива	Национално германско								НАТО					
	Restricted /За служебно ползване/		Confidential /Поверително/		Secret /Секретно/		Top secret /Строго секретно/		Restricted /За служебно ползване/		Confidential /Поверително/		Secret /Секретно/	
Интеграция	LAN	VAN	LAN	VAN	LAN	VAN	LAN	VAN	LAN	VAN	LAN	VAN	LAN	VAN
Темпест	Без зона		Зона 1				Зона 0		Без зона		Зона 1		Зона 0	
Антитампер	Не		да						Не		да			
Галваническо разделение	не		Да						не		Да			
Симетрично криптиране	≥AES		≥XIA		≥XIA		Libelle		≥AES		Libelle			

**Благодаря за вниманието!**

- ТЕЛЕСПРИНТ 90 ООД - secunet Security Networks AG
- Telefon: 029200001
- E-Mail: [telesprint@telesprint.com](mailto:telesprint@telesprint.com)

