

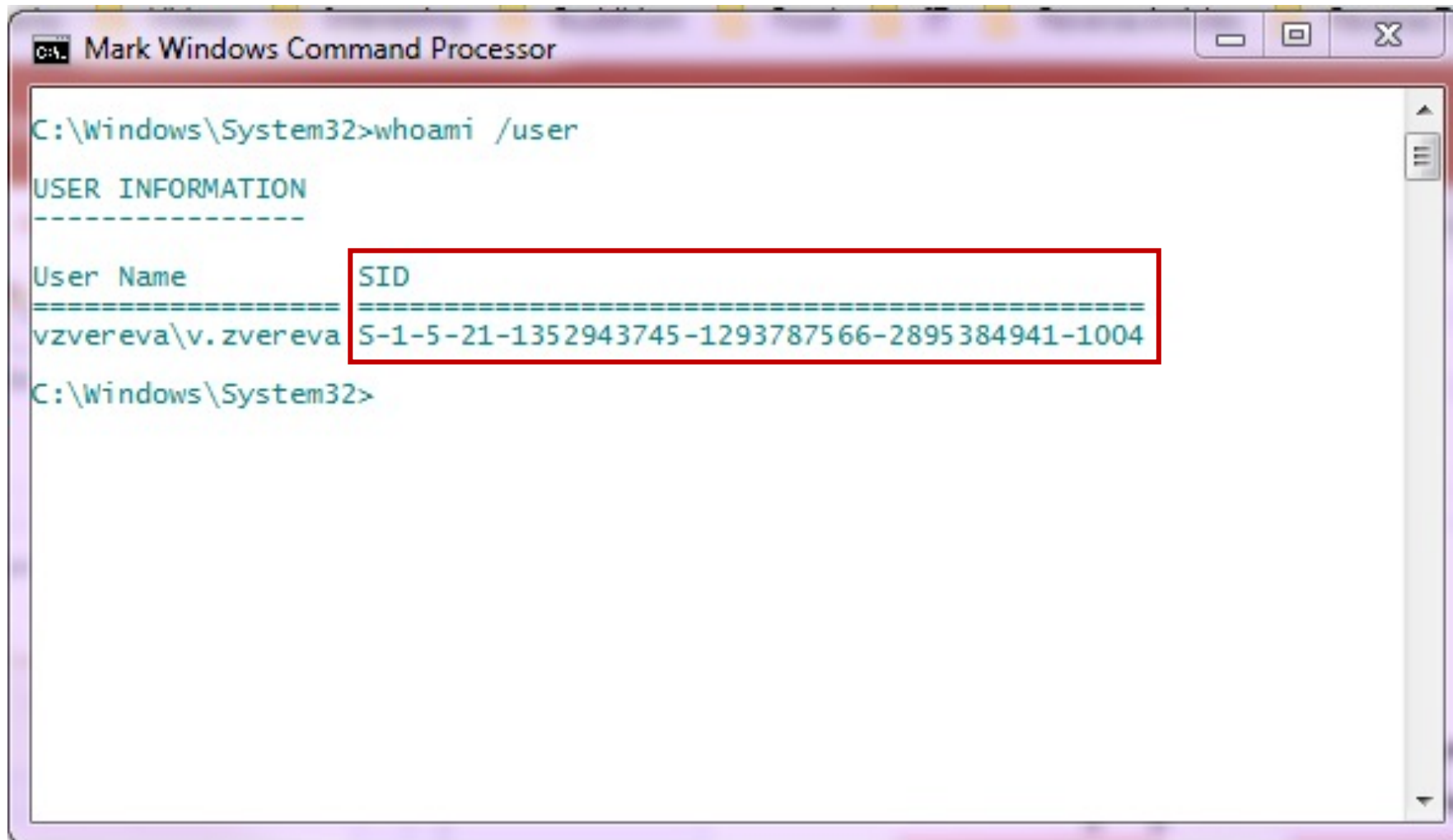
Вход в систему: ВЗГЛЯД ИЗ-ЗА КУЛИС



Содержание

- SID/RID - Security ID/Resource ID
- Типы входа в систему
- LSA – Local Security Authority

SID - идентификатор безопасности



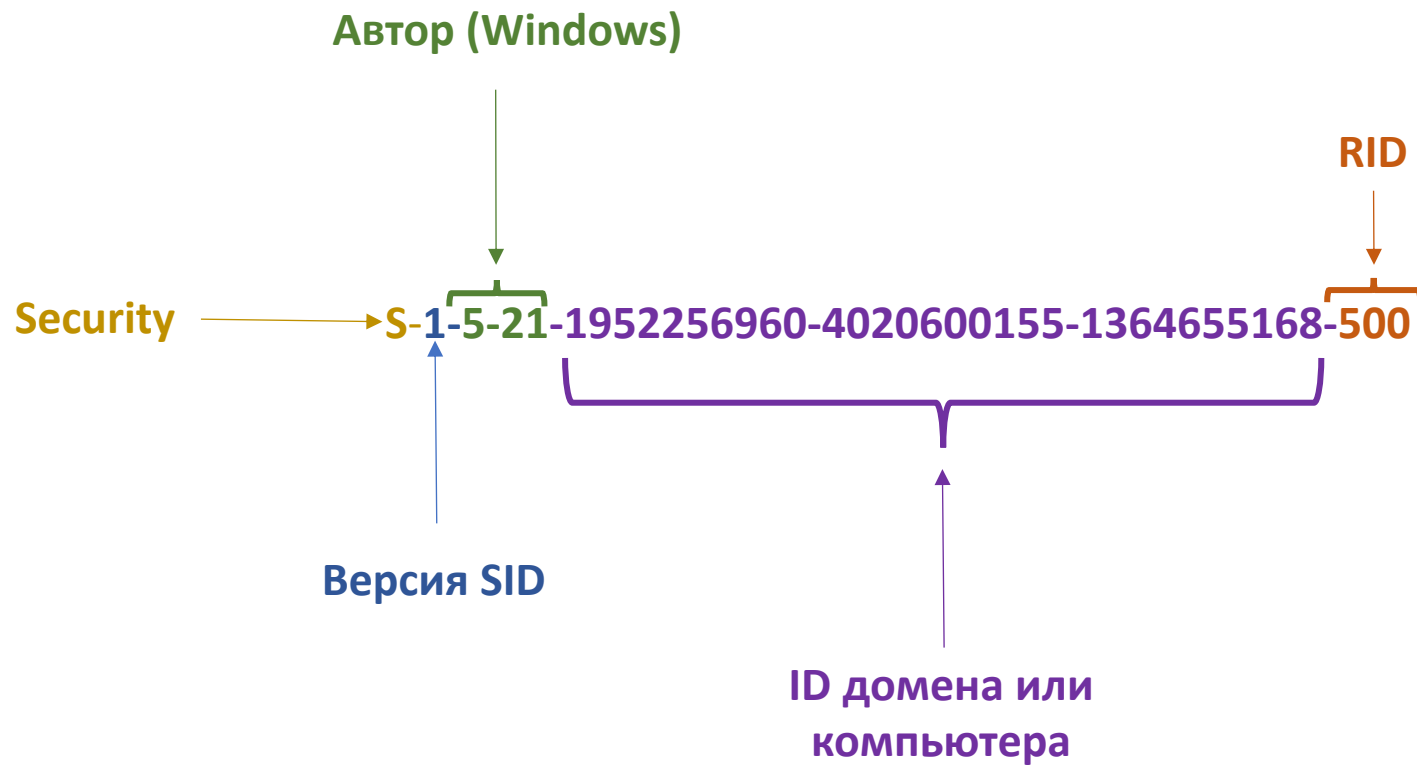
```
C:\Windows\System32>whoami /user

USER INFORMATION
-----

User Name      SID
=====
vzvereva\v.zvereva S-1-5-21-1352943745-1293787566-2895384941-1004

C:\Windows\System32>
```

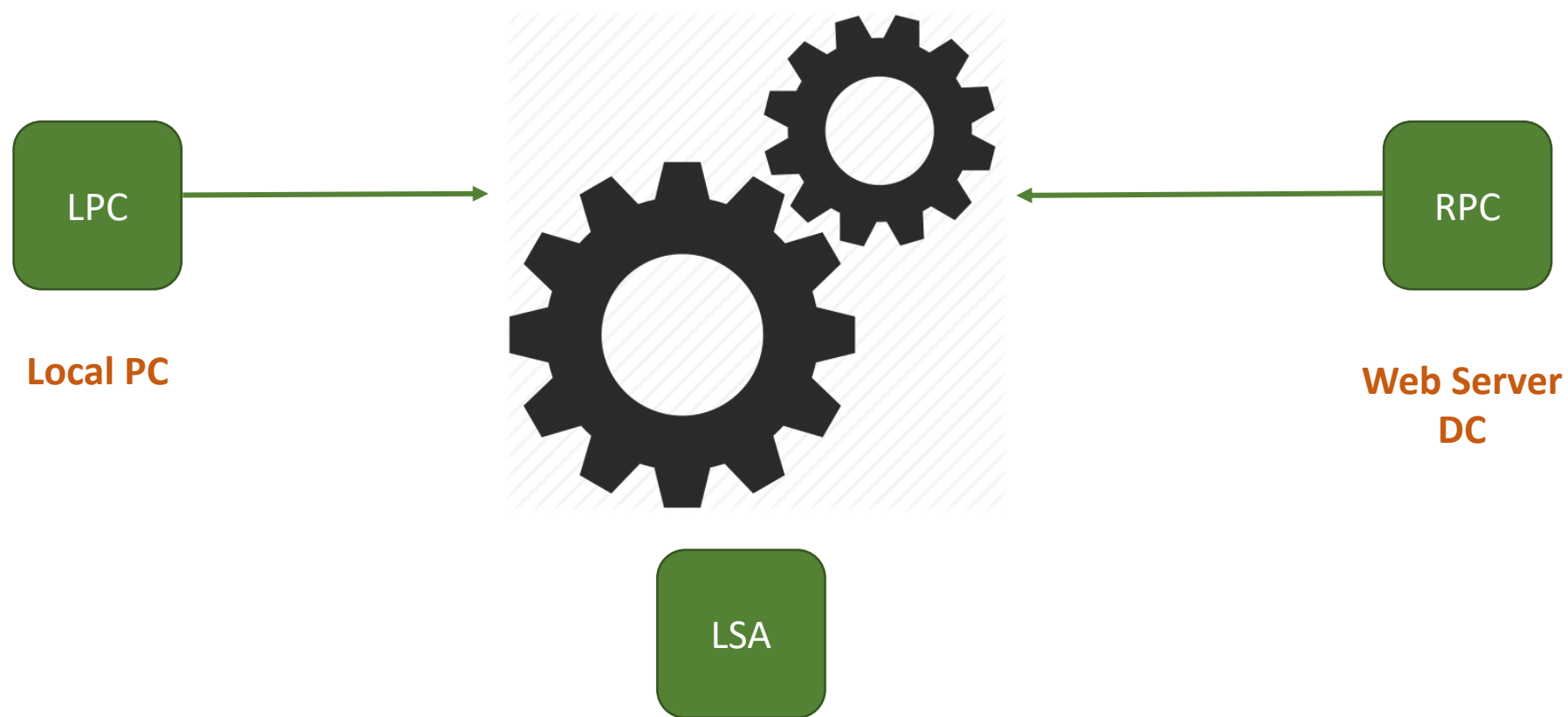
SID - идентификатор безопасности



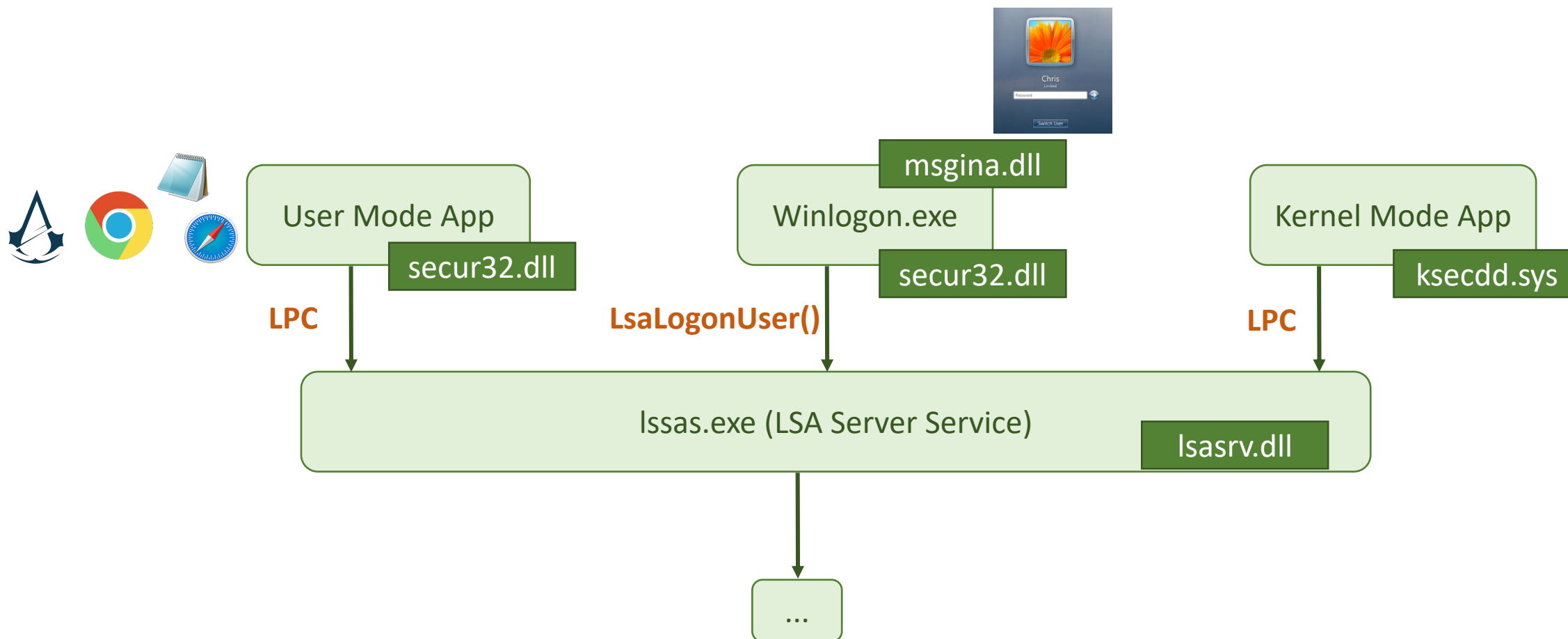
SID - примеры

- S-1-5-21-X-X-X-500 - встроенный admin
- S-1-5-21-X-X-X-500 - встроенный guest
- S-1-5-21-X-X-X-1000 - первый созданный пользователь
- S-1-5-18 - System
- S-1-5-3 - batch
- S-1-5-2 - network
- S-1-5-21-544- группа локальных администраторов

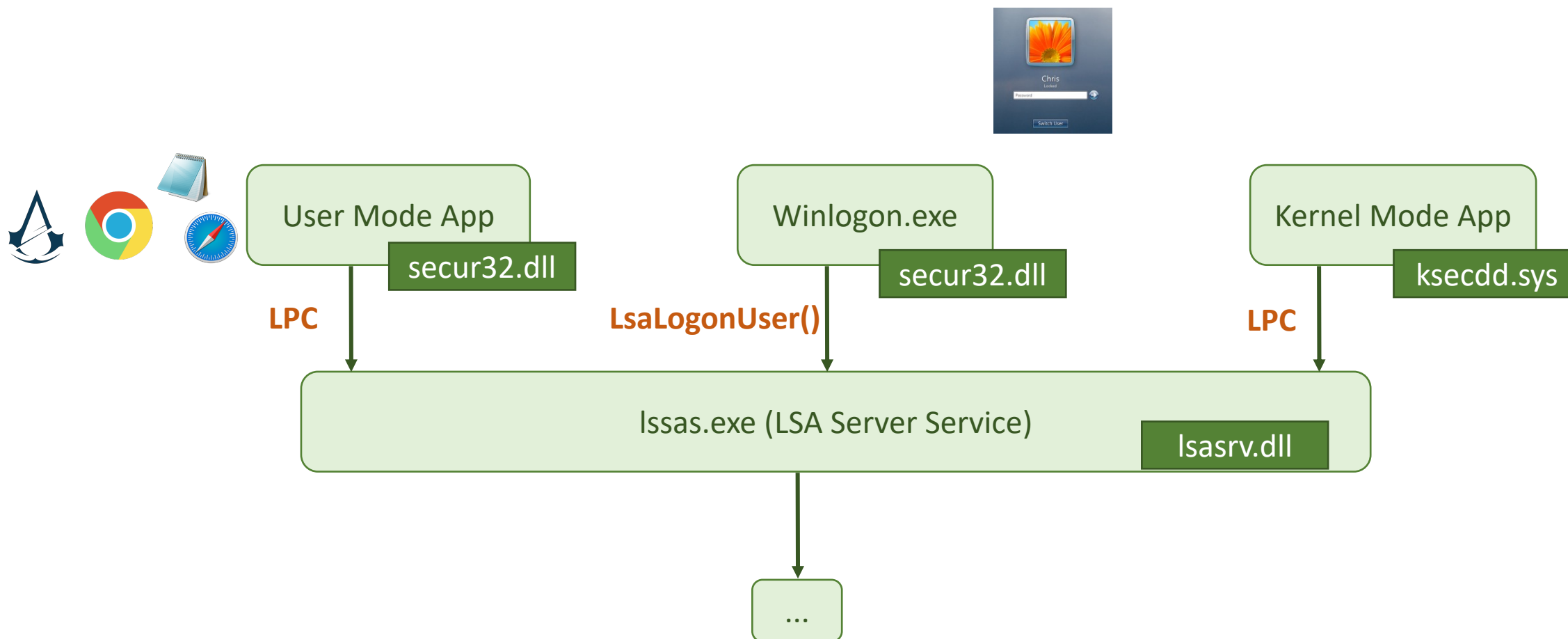
Вход в систему



Вход в систему (до Vista)

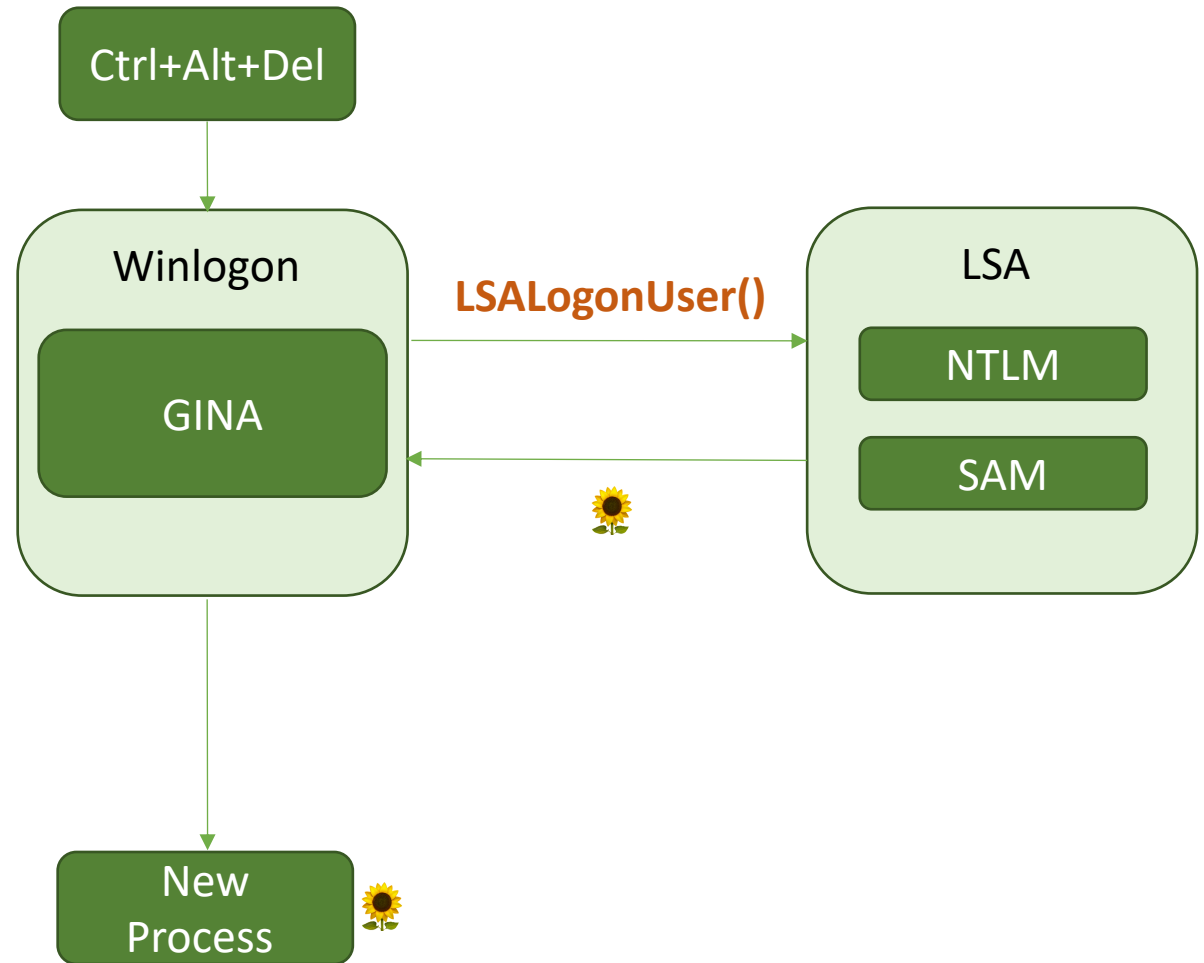


Вход в систему (после Vista)



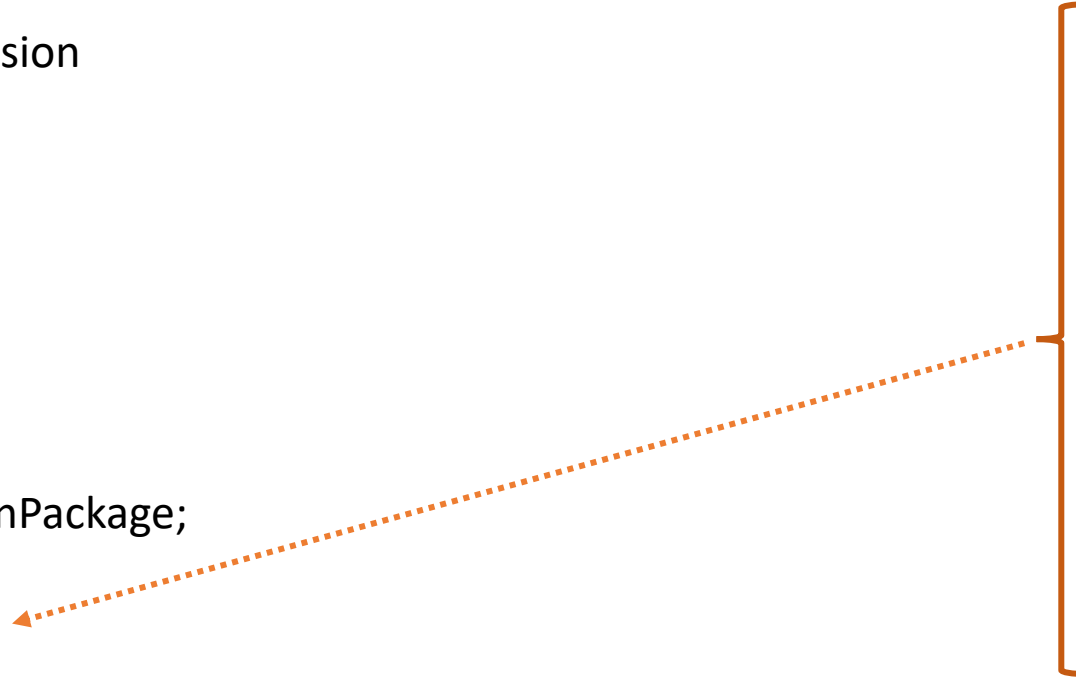
Типы входа

0. Система
1. ???
2. Интерактивный
3. Сетевой
4. Task manager/batch
5. Сервис
6. Proxy
7. Разблокировка
8. Network clear text
9. Новый пользователь
10. RDP
11. Кэш



Win32_LogonSession class

```
class Win32_LogonSession
{
    string Caption;
    string Description;
    datetime InstallDate;
    string Name;
    string Status;
    datetime StartTime;
    string AuthenticationPackage;
    string LogonId;
    uint32 LogonType;
};
```

- 
- 0. Система
 - 1. Нет информации
 - 2. Интерактивный
 - 3. Сетевой
 - 4. Task manager/batch
 - 5. Сервис
 - 6. Proxy
 - 7. Разблокировка
 - 8. Network clear text
 - 9. Новый пользователь
 - 10. RDP
 - 11. Кэш

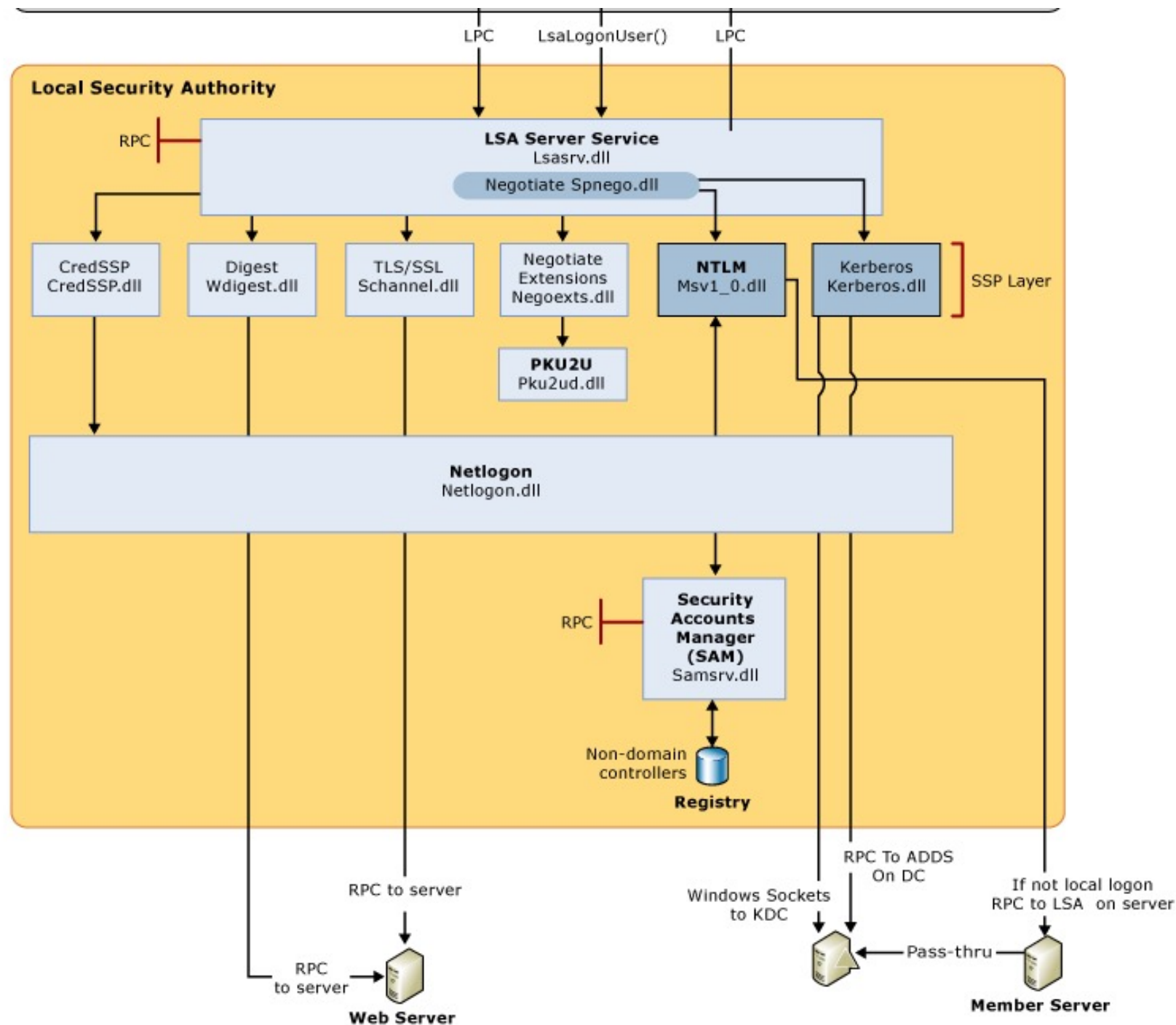
LsaLogonUser (Secur32.dll)

```
NTSTATUS LsaLogonUser(  
    HANDLE          LsaHandle,  
    PLSA_STRING      OriginName,  
    SECURITY_LOGON_TYPE LogonType,  
    ULONG            AuthenticationPackage,  
    PVOID            AuthenticationInformation,  
    ULONG            AuthenticationInformationLength,  
    PTOKEN_GROUPS     LocalGroups,  
    PTOKEN_SOURCE      SourceContext,  
    PVOID             *ProfileBuffer,  
    PULONG            ProfileBufferLength,  
    PLUID             LogonId,  
    PHANDLE           Token,  
    PQUOTA_LIMITS      Quotas,  
    PNTSTATUS          SubStatus  
);
```

Click to add text

Username + Password

Local Security Authority



GINA (msgina.dll)



Lsass.exe

%WINDIR%\System32

lsass.exe	0.12	5 108 K	12 208 K	492 Local Security Authority
csrss.exe	0.01	2 496 K	4 384 K	500 Служба диспетчера ло
conhost.exe	0.02	2 416 K	6 104 K	400 Процесс исполнения
winlogon.exe		1 604 K	5 796 K	232 Окно консоли узла
explorer.exe		2 768 K	7 008 K	436 Программа входа в си
VBoxTray.exe	0.07	76 456 K	98 876 K	1388 Проводник
cmd.exe	0.04	2 916 K	8 220 K	1060 VirtualBox Guest Additio
Procmon.exe		1 996 K	2 960 K	3008 Обработчик команд W
Procmon64.exe		4 328 K	11 864 K	3484 Process Monitor
procexp64.exe		18 436 K	29 756 K	1764 Process Monitor
jusched.exe	1.67	24 944 K	33 684 K	1972 Sysintemals Process Ex
		5 004 K	11 156 K	1876 Java Update Scheduler

Name	Description	Company Name	Path	Verified Signer
logoncli.dll	Net Logon Client DLL	Microsoft Corporation	C:\Windows\System32\logoncli.dll	(Verified) Microsof...
lsasrv.dll	Библиотека DLL сервера LSA	Microsoft Corporation	C:\Windows\System32\lsasrv.dll	(Verified) Microsof...
lsasrv.dll.mui	Библиотека DLL сервера LSA	Microsoft Corporation	C:\Windows\System32\ru-RU\lsasrv.dll.mui	(Verified) Microsof...
lsass.exe	Local Security Authority Process	Microsoft Corporation	C:\Windows\System32\lsass.exe	(Verified) Microsof...

Спасибо за внимание!

