

Giving Permissions through Stored Procedures

Erland Sommarskog
SQL Server MVP

SQLSat Kyiv Team



Eugene Polonichko



Alesya Zhuk



Yevhen Nedashkivskyi



Oksana Tkach

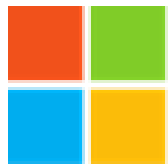


Mykola Pobyivovk



Oksana Borysenko

Our Awesome Sponsors



Microsoft



intapp™



DB-BEST
TECHNOLOGIES

eleks®



devart
Database Interaction Solutions

DATAART

infopulse

<epam>

DIGITALUKRAINE



доставка
крафтового
пива

Session will begin very soon :)

Please complete the evaluation form from your pocket after the session. Your feedback will help us to improve future conferences and speakers will appreciate your feedback!

Enjoy the conference!

A photograph of a dirt path winding through a lush forest. The path is covered in fallen leaves and is flanked by dense green ferns and other foliage. In the background, tall pine trees stand against a bright sky. A small blue and white sign is visible on the left side of the path.

Erland Sommarskog

Independent consultant based in Stockholm

SQL Server MVP since 2001

<http://www.sommarskog.se>

esquel@sommarskog.se

Giving Permissions through Stored Procedures

If a user has permission to run a stored proc,
does he need permission for any action
performed inside the stored procedure –
YES or NO?

YES in some common cases –
but the general answer is **NO**.

In this session we will learn how we can make
the statement become YES in general.

Agenda

- Ownership Chaining
- Certificate Signing
- The EXECUTE AS Clause
- The Dangers of TRUSTWORTHY

Slides and all scripts are available on
<http://www.sommarskog.se/present>

Ownership Chaining

No permissions are checked when a module (procedure, view, function or trigger) accesses an object with the same owner. Applies to:

- DML (SELECT, INSERT, UPDATE, DELETE & MERGE).
- Execution of stored procedures and functions.

Does not apply to:

- Dynamic SQL.
- Metadata access.
- Special permissions such as ALTER.

Certificate Signing

The recipe:

1. Create a certificate.
2. Sign the procedure with the certificate.
3. Create a user from the certificate.
4. Grant the certificate user the permissions needed (which could be role membership).

When something is signed with a certificate, this permits you to verify that the contents is unchanged using only the public key.

What is this User?

This is a special type of user that exists only to connect permissions and certificate. It cannot log in or be impersonated.

You can only create one user per certificate.

When the procedure has a valid signature, the token of the certificate user is added to `sys.user_token`, just like a role.

Net effect: the permissions of the certificate user are added to the user's own permissions.

Observations on Certificate Signing

Procedure must be signed after each change.

The token and thus the permissions of the certificate user are carried on to dynamic SQL and system procedures.

But they are **not** carried on to nested procedures, triggers or functions.

Keep in mind: DENY always trumps GRANT.

Certificate Management

Each procedure with need of special permissions has its own certificate, granted exactly the permissions needed – the principle of minimum permissions.

You can have a special stored procedure that performs the signing. If developers are trusted, this procedure can be called from the deployment script for the stored procedures.

The password? Throw it away!

Server-Level Permissions, when in master

1. Create a certificate in the master database.
2. Sign the procedure with certificate.
3. Create a login from that certificate.
4. Grant the login the required permissions.

While called “login”, this login cannot log in – it exists only to connect permissions and certificate.

Tokens can be inspected in `sys.login_token`.

Server-Level Permissions in User DB

1. Create a certificate in the master database.
2. Create a login from the certificate.
3. Grant the login the required permissions.
4. Export certificate.
5. Move to user database.
6. Import certificate.
7. Sign the procedure.
8. Optional: drop private key.

Export/Import Certificate

In all versions (from SQL 2005 and up):

- Export: **BACKUP CERTIFICATE** (to disk).
- Import: **CREATE CERTIFICATE FROM FILE** (and delete the file).

In SQL 2012 and later:

- Export: **certencodded()** and **certprivatekey()**.
- Import: **CREATE CERTIFICATE FROM BINARY**.

What About Availability Groups?

In an AG, certificate, login and permissions must exist on all nodes in the AG, so that things can work after a failover.

Big hassle? Don't worry, I have a script for you:

- Creates cert and login and grants permissions in master.
- Exports the cert to the user database and signs the procedure.
- For AGs: Loops over the other nodes in the AG, using a temporary linked server to copy cert, login and permissions.
- You must specify: database, procedure and permissions.

EXECUTE AS and DB Permissions

Proper version:

1. Create a proxy user **WITHOUT LOGIN** with the name derived from the procedure.
2. Grant the proxy user the required permissions.
3. Add the clause
`WITH EXECUTE AS 'SPName$Proxy'.`

User creation and granting are in the same file as the procedure.

Lazy version:

1. Use `WITH EXECUTE AS OWNER` and no proxy user.

EXECUTE AS, cont'd

A lot simpler than certificates. ...but!

- Lazy version breaks the principle of granting minimum permissions.
- Breaks schemes for row-level security and auditing based on SYSTEM_USER, USER etc.
- This can be mitigated by using original_login() or context_info/session_context – requires planning ahead.
- If your system is not ready for EXECUTE AS – you can stop it with a DDL trigger.

Server-Level Permissions and EXECUTE AS

Create a proxy login, grant permissions, add EXECUTE AS clause?

[10_execasserver.sql](#)

When impersonating a **database user**, we are sandboxed into the current database and cannot access things outside it, unless two doors are opened:

1. The database must be set **TRUSTWORTHY**.
2. The database owner must have been granted the permission **AUTHENTICATE SERVER**.
(Which is the case if owner = sa.)

[11_trustworthy1.sql](#)

TRUSTWORTHY is a Security Risk

With certificate signing, the DBA can request to review the code every time an application admin wants to change an SP with server-level access.

EXECUTE AS + TRUSTWORTHY gives the application admin carte blanche to change the SP to his/her own liking.

But that is not all. Danger alert!

[12_trustworthy2.sql](#)

Combined with AUTHENTICATE SERVER, a person with **db_owner** rights (or rights to create and impersonate users) can elevate to **sysadmin**.

TRUSTWORTHY, cont'd

Recommendation: the owner of each database should be a unique SQL login which exists solely to own that database.

Hopefully, you think twice before you grant that login `AUTHENTICATE SERVER` to open the second door.

It is OK to open both doors, **IF** everyone with permission to create users in the database already are sysadmin.

...and this will never change. (Think: consultants.)

Recap: Ownership Chaining

What you use 95% of the time, for plain and simple DML in stored procedures.

- Does not work with dynamic SQL.
- Does not work with “advanced” permissions.
- Does not work with metadata.
- Does not work with server-level permissions.

Recap: Certificate Signing

Permits you to grant about any database or server permission through stored procedures in a fine-grained way. (But cannot overcome an explicit DENY.)

Seems to be a bit of hassle at first, but with organisation and throw-away passwords it's not a big deal.

The preferred method for database permissions.

Always use certificates for server-level permissions!

Recap: EXECUTE AS

Good for the lazy and casual. :-)

Implications for auditing and row-level security that requires you to plan ahead.

Can be OK for database permissions if conditions are relaxed (or you need to overcome DENY).

Always use certificate signing for server-level permissions!

It's Getting Very Near the End...

Erland Sommarskog – esquel@sommarskog.se

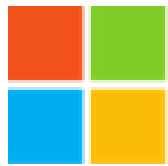
Scripts and slides on
<http://www.sommarskog.se/present>

Giving Permissions through Stored Procedures on the web:

<http://www.sommarskog.se/grantperm.html>

...and beware of TRUSTWORTHY!

Our Awesome Sponsors



Microsoft



intapp™



DB-BEST
TECHNOLOGIES

eleks®



devart
Database Interaction Solutions

DATAART

infopulse

<epam>

DIGITALUKRAINE



доставка
крафтового
пива