Credentials Mini-Guide

ID Cards for Your Digital Tools

bleen42.com

Imprint / Legal Notice

Author & Publisher:
Dr. Christa Gescher (Dr. phil.)
c/o IP-Management #4973
Ludwig-Erhard-Straße 18
20459 Hamburg, Germany

Contact:
Email: connect@bleen42.com
Website: https://www.bleen42.com

This guide was created with the assistance of artificial intelligence tools for research and initial drafting, followed by human editing for accuracy and organization. While every effort has been made to ensure reliability, AI-generated content may contain errors or omissions.

Disclaimer:
This guide is for informational purposes only. The author and publisher disclaim any liability for actions taken based on the content. Results may vary. Readers should consult relevant professionals as needed.

Table of Contents

When You Connect Tools 4
What This Guide Covers 4

Identity and Permissions 5
How Credentials Work 5

Understanding the Roles 6
Tool Roles: Origin and Target 6
Your Role 7

Types of Credentials 8
API Key 9
OAuth (Open Authorization) 10
Token 11
Webhook 12

How Data Flows 13
Pull Pattern: The Target Asks for Data 13
Push Pattern: The Origin Sends Data 13

Managing Your Credentials 14
Naming Best Practices 14
Two-Factor Authentication (2FA) 14
Removing or Resetting Credentials 15
Troubleshooting Tips 15
Storing Credentials Safely 16

You're All Set 17

When You Connect Tools

If you are working with tools to create a website, shopping platform, emails, automations, or anything else digital, you have likely encountered requests for "credentials," "authorization," or "API keys" when trying to connect the tools.

These requests appear whenever you want to connect tools in an automation or workflow, e.g., connecting your email to Google Workspace, or using a ChatGPT agent or n8n to link different tools. They point to credential systems that are designed to protect your information and give you control over how your tools work together and what data they share.

What This Guide Covers

This guide, written from a non-tech perspective, is a bird's eye overview of credentials to help you understand what they are, how they work, and how to use them to establish stable connections between your tools. It gives you a clear picture of your role in these workflows and shows you what to do when a tool asks for a key, an approval, or a webhook URL.

Identity and Permissions

When you connect two tools, e.g., Zapier to your Google Sheets, the credential system needs to verify two things to keep your data protected:

1. **Your identity**: Is your account actually authorizing this connection, or is someone else pretending to be you?
2. **Permissions you grant**: Can the tool read your data? Edit it? Delete it?

Credentials prove identity (called "authentication") and define permissions (called "authorization").

How Credentials Work

When you open an account (e.g., a Google account), you create a password. This is your personal password that you should never share, not even with other tools. Because of this reason, tools use credentials to establish secure connections. These credentials identify your account, prove that you authorized the connection, and specify exactly what the tool can access — all without using your password. This way, credentials create a secure bridge between tools.

Understanding the Roles

Before you connect anything you want to understand what roles the tools are playing and what your own role is.

Tool Roles: Origin and Target

When connecting tools they take specific roles:

- **Source/Sender** = the place where the event happens or where the data lives (called "origin" in this guide). The origin either sends data on request or holds data that a target will fetch.
- **Receiver/Doer** = the tool that receives data or performs an action with that data (called "target" in this guide). It asks for data actively or accepts incoming data and does something with it.

Note: Depending on the tool, you might see different word pairs for the two sides of a connection, such as Origin–Target, Source–Destination, Sender–Receiver, Service to connect from–Service to connect to, Trigger–Action, Service Provider–Client, Resource Server–Requester, or Integration Source–Integration Target.

No matter which terms appear, they always refer to where data starts (term on the left = "origin") and where it goes or what happens with it (term on the right = "target").

Your Role

Usually, the tools you want to connect will actively prompt you to do something. You simply click, copy, paste, or allow. The rest happens automatically.

Common Prompts:

- "Authorize this app"
- "Grant permissions" or "Allow access"
- "Connect with [Tool Name]"
- "Sign in to authenticate"
- "Create API key" or "Generate new key"
- "Copy webhook URL"
- "Paste your API token here"
- "Select permissions" (with checkboxes for read/write/delete)

Tip: Take Screenshots

When you successfully find a credential or complete a connection, you may want to take a quick screenshot of the settings page where the credential was located and how you navigated there. This makes it much easier to find the same credential again later or troubleshoot if something goes wrong.

Types of Credentials

Think of credentials as identity documents:

- **API Key**: Long-term identity, like an ID card or passport — proves who you are, doesn't expire until you delete it manually
- **OAuth**: Permission-based and temporary, like a visitor pass or visa — granted for specific purposes, expires, can be revoked
- **Token**: Short-lived and task-specific, like a security badge for a restricted area — works for a limited time
- **Webhook**: Like a mailing address — you give it out so others know exactly where to send their letters; it’s your address until you move out.

API Key

What it is: A long character string that confirms your identity in the origin tool, which the target tool requires before you can connect them.

How it works: Like a passport number identifies you as a person, an API key identifies your account in your origin tool. When you want to connect from your origin tool to a target tool, the target will ask you for the origin tool's API key.

Where to find it: In the settings or developer section of the origin tool.

Security: Store your API key somewhere safe (e.g., in a password manager or another secure location), because anyone who has this key could potentially access your origin tool account.

Duration: The API key provides the target tool with a permanent key that works until you manually delete it. It's like giving someone a copy of your house key.

OAuth (Open Authorization)

What it is: A connection method where you grant temporary, limited permission to the target tool. Unlike API keys, you don't copy or paste anything, OAuth is a process that guides you through the connection.

How it works: Like a visa that grants a temporary stay, OAuth allows temporary access for the target tool to reach the origin tool that holds the data. The target starts the process by asking you to sign in to the origin tool (this step is called "Redirect") to allow access. The target tool then asks what permissions you'll grant it (e.g., read, edit, delete data in the origin tool). If the OAuth connection expires, you'll see a notification and only need to click "Reconnect" to re-establish it.

Duration: You grant only temporary, limited permission that expires automatically. It's like giving someone a visitor pass to your house for a certain period of time, and only to certain rooms.

Token

What it is: A token is short-lived digital pass that allows the target tool to access the origin tool's data for a brief period. There are two common token types: *access token* (a short-term pass) and *refresh token* (a renewal slip that allows the target to get a new access token without you signing in again).

How it works: When connecting, the target asks for a token. The origin then provides the target with an access token so the target can call the origin's API. Access tokens expire quickly for safety; if the target needs continued access, it proactively uses a refresh token to ask the origin for a new access token.

Important note: While most of the time you won't be asked to manage tokens, there are situations when a token (or token-like secret) will be shown to you and you'll be asked to save it. When you see a message saying "This is the only time you will see it," copy and save the token immediately in your password manager. You may need it later to verify your connection, set up the same integration elsewhere, or troubleshoot connection issues.

Webhook

What it is: A webhook is a push mechanism that lets the origin send data to the target the moment an event happens (e.g., a Typeform submission, a Calendly booking, or a ChatGPT Agent triggering a workflow).

How it works: The target (e.g., n8n or Make) provides a webhook URL when you create a Webhook/Trigger node. You copy that URL and paste it into the origin's Webhook/Endpoint settings.

Think of the webhook URL as the target's mailbox: the origin drops the message there; the target reads it and acts.

How Data Flows

Pull Pattern: The Target Asks for Data

When you connect via the pull method, the target (e.g., n8n) asks the origin (e.g., Google Sheets) for access to fetch ("pull") data or perform an action on it. In this case, the target n8n prompts you to either paste the API key from the origin Google Sheets or click "Connect with Google" (OAuth) so it can access the data in the sheets.

Push Pattern: The Origin Sends Data

When you connect via the push method, the origin (e.g., an email opt-in form) actively sends ("pushes") the data to the target (e.g., n8n). In this case, your job is to prepare the origin by telling it when to send the data and where to send it. You do this by copying the webhook URL from the target and pasting it into the origin (e.g., the form submission tool).

Managing Your Credentials

Naming Best Practices

When you create or save a credential in a tool, it is recommended to name it clearly so you'll remember what it is and where it is used, e.g. by adding the tool name (e.g., Google), purpose (e.g., Sheets), and owner (your initials or email address) to the name.

Two-Factor Authentication (2FA)

Some tools, especially for important accounts like email or banking, add an extra security step called two-factor authentication, or 2FA, to protect your credentials. You have the option to set up 2FA to provide a second proof (like a code from your phone) when signing in or connecting tools. 2FA is like showing two forms of ID instead of one, to add extra security to your accounts.

Removing or Resetting Credentials

If you want to change a tool, suspect a problem, or simply want to tidy up your connections, you can always remove or reset credentials. Most tools let you delete a credential directly from the settings or connections area. If a credential is compromised, it is advised to delete or regenerate it immediately to keep your data safe.

Troubleshooting Tips

Things to try when a connection doesn't work:

- Make sure the credential hasn't expired (OAuth connections often do)
- Reconnect the tool if asked, especially when you see an "expired" or "invalid" error message
- Double-check permissions: sometimes you need to allow read, write, or specific access for the connection to work
- If all else fails, delete the old credential and create a new one — this often fixes things quickly

Storing Credentials Safely

It is advised to keep your credentials somewhere secure, such as in a password manager. Other good options include encrypted documents or notes saved locally or on a secure drive (with strong passwords), using an encrypted USB stick, or maintaining a handwritten logbook stored in a locked location.

Credentials are powerful and sensitive, they open doors to your data. Never share them publicly (for example, in a screenshot or in a support forum).

Treat them the way you would treat the keys to your house, and only let trusted people access them.

You're All Set

You have explored the essentials of credentials: what they are, how they work, and how to manage them safely. Now you have a good foundation to decide your next step or to know where to dig deeper.

Enjoy, and happy connecting!