PasswordRadar

Password screening attestation

Issued by **KnownPass s.r.o.**, operator of PasswordRadar, Czech Republic

Statement. KnownPass s.r.o., the operator of PasswordRadar, attests that in the period the service answered 30,835 range lookups made with the 3 API keys of Acme Example s.r.o. It answered lookups on every one of the period's 92 days, from the base dataset and the Czech, Slovak and German language packs. The service cannot see what the customer's systems did with the answers; section 4 lists that evidence and who holds it.

Attestation number	`PR-ATT-2026Q3-SAMPLE`
Date of issue	**6 October 2026**
Period covered	**1 July to 30 September 2026** UTC
Customer	**Acme Example s.r.o.** fictional
Customer domain	`acme.example`
Plan in the period	**Team**

1 API keys and lookups answered

Every API key on the account during the period.

Key ID	Answered lookups per day (Jul | Aug | Sep)	July	August	September	Period	Days with lookups
`a41c09e2` Issued 8 June 2026		9,435	8,927	9,945	28,307	92 of 92
`7be25c14` Issued 17 August 2026		–	775	1,600	2,375	45 of 45
`5d7e3b10` Issued 27 April 2026 Revoked 2 September 2026		118	35	0	153	13 of 64
All keys		**9,553**	**9,737**	**11,545**	**30,835**	**92 of 92**

- A range lookup is one request to `GET https://api.knownpass.com/v1/range/{prefix}` that the service answered with the hashes in that bucket. Counts come from the per-key daily counts kept for invoicing; this document holds no per-request records, hash prefixes or passwords.
- Days with lookups: days with at least one answered lookup, out of the days the key was active. Lookups happen only when a password is set, changed, reset or entered, so a quiet day is not by itself a gap. Each strip is scaled to its key's busiest day; a dash means the key was not active that month.
- Service incidents recorded on the status page in the period: 29 September 2026, 02:10 to 02:52 UTC, range lookups unavailable (42 minutes). Marked ▮ in the strips. Bulk downloads by the account's keys: none. Lookups against a self-hosted copy of a dataset never reach the service and are not counted here.

2 Datasets that answered

All 3 keys were entitled to these 4 datasets while active.

Dataset	Versions in service (Jul | Aug | Sep)	Categories	Version and its days in service
Base dataset		Website leaks, Malware leaks, Password lists, Wordlists, Common, Masks & patterns, Brute-force space (every printable string of 1 to 5 characters)	`2026.06.29` until 2 August `2026.08.03` 3 August to 30 August `2026.08.31` from 31 August
Czech language pack		Czech wordlists	`2026.05.18` whole period
Slovak language pack		Slovak wordlists	`2026.05.18` until 9 August `2026.08.10` from 10 August
German language pack		German wordlists	`2026.05.18` whole period
Tailored dataset	None	Generated from a domain	None in the period

3 What the service receives

Received with each lookup

- **A 6-character hash prefix:** the first 6 hex characters of `SHA-1("Salted for knownpass.com: " + password)`. It selects one of 16,777,216 buckets, each holding hundreds of hashes.
- **The API key,** which identifies the account, not a person.
- **The calling server's IP address** and ordinary HTTPS metadata.

Never received

- **The password,** in any form.
- **The full hash.** The customer's server compares it with the returned bucket, so the service does not learn whether a password matched.
- **Usernames, email addresses or user IDs.** The API has no field for them.

Run in the EU by KnownPass s.r.o., a Czech company. The salt and the API host keep the original name: knownpass.com is the company's domain, and PasswordRadar was called knownPass.

4 What this attestation does not cover, and the evidence the customer keeps

Question an auditor may ask	From this attestation	From the customer's own records
Was a screening service in use, and by which systems?	Section 1: keys, lookups per month and days with lookups.	A record of which system and environment uses each key ID.
What were passwords screened against, and how current was it?	Section 2: datasets, categories and versions in service.	Nothing further needed.
Did passwords or full hashes leave the customer's systems?	Section 3: what the service receives.	The client code or configuration that hashes locally and sends only the 6-character prefix.
Is the check called whenever a password is set, changed or reset?	Not visible to the service.	The code or configuration of each flow, and a periodic test that a known leaked password is refused in each one.
Were matching passwords refused?	Not visible to the service: the comparison runs on the customer's server.	A log entry for each refused password with the time, the flow and the category returned. Never the password, its hash or the prefix.
What happened when the check could not run?	Section 1: service incidents in the period (one, on 29 September 2026).	A log entry for each skipped check (timeout, network error, 429, 5xx) or failed one (400, 401, 403, other errors), and the re-check at the next login or password change.
Are organisation-specific words blocked (company name, products, places)?	Section 2: no tailored dataset on this account, so the service did not cover this.	The customer's own blocklist, if it keeps one.
How are passwords stored, is MFA in place, and what does the access-control policy say?	Outside the scope of this attestation.	The customer's own controls and policy documents.

Kept together, this attestation and those records cover both halves of the control: current screening data was available and queried, and the customer acted on the answers.

5 How this maps to requirements Informational, not legal advice.

Reference	What it covers, in short	Where this attestation helps
NIST SP 800-63B-4 (August 2025), section 3.1.1.2	When a password is set or changed, the verifier SHALL compare it against a blocklist of commonly used, expected or compromised passwords. Context-specific words, such as the name of the organisation or the service, are named as blocklist material.	Sections 1 and 2 show which blocklist was in use and that it was queried. The comparison and the refusal are shown by the customer's records (section 4).
NIS2: Directive (EU) 2022/2555, Article 21(2)(g) and (i)	Cybersecurity risk-management measures include basic cyber hygiene practices (g) and access control policies (i).	Supports evidencing password screening as part of these measures.
Czech Republic: Act No. 264/2025 Sb. on Cybersecurity	In force since 1 November 2025, supervised by NÚKIB. Security measures are set by Decree No. 409/2025 Sb. (higher obligations) and Decree No. 410/2025 Sb. (lower obligations).	Supports evidencing password-screening and access-control measures under the decree that applies.
Czech decrees: No. 409/2025 Sb., § 19(4), and No. 410/2025 Sb., § 8(4)	For accounts that still rely on a password alone, the password tool must enforce at least 12 characters for users, 17 for administrators and 22 for technical accounts; a change at least every 18 months; no reuse of the last 12 passwords; no simple and commonly used passwords, or ones based on repeated characters, the login name, email address or system name.	Supports evidencing the check against simple and commonly used passwords (sections 1 and 2). The other rules are the customer's own controls.
Slovakia: Act No. 69/2018 Coll. on Cybersecurity as amended by Act No. 366/2024 Coll.	In force since 1 January 2025, supervised by NBÚ.	Supports evidencing password-screening and access-control measures.

None of these texts requires PasswordRadar or any other specific product. Whether the customer's measures meet an obligation is for the customer and its auditor to assess.

This attestation is KnownPass s.r.o.'s statement of its own service records for the period. It is not an audit, a certification or an assurance report. It is issued to the customer, who may share it with its auditors and supervisory authority; no one else may rely on it. Liability follows the terms of service in force for the period.

Issued by

KnownPass s.r.o.
Operator of PasswordRadar
Czech Republic
hello@passwordradar.eu

Signed for the issuer

Sample, not signed

Šimon Podlesný
Executive director (jednatel),
KnownPass s.r.o.
6 October 2026

Checking that an attestation is genuine

1. Compute the SHA-256 of the PDF exactly as received: `sha256sum` on Linux, `shasum -a 256` on macOS, `certutil -hashfile <file> SHA256` on Windows.
2. Email the attestation number and the hash to hello@passwordradar.eu.
3. We reply whether both match our register of issued attestations. This sample is not in the register.